Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

2021-09

LEVERAGING DHS ASSETS: POTENTIAL FOR THE TRANSPORTATION SECURITY ADMINISTRATION TO ENHANCE U.S. GOVERNMENT INTELLIGENCE CAPABILITIES

Zeigler, Zachary D.

Monterey, CA; Naval Postgraduate School

http://hdl.handle.net/10945/68400

Copyright is reserved by the copyright owner.

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

LEVERAGING DHS ASSETS: POTENTIAL FOR THE TRANSPORTATION SECURITY ADMINISTRATION TO ENHANCE U.S. GOVERNMENT INTELLIGENCE CAPABILITIES

by

Zachary D. Zeigler

October 2021

Co-Advisors: Cristiana Matei
Paul J. Smith (contractor)

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** October 2021	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE LEVERAGING DHS ASSETS: POTENTIAL FOR THE TRANSPORTATION SECURITY ADMINISTRATION TO ENHANCE U.S. GOVERNMENT INTELLIGENCE CAPABILITIES	**5. FUNDING NUMBERS**
6. AUTHOR(S) Zachary D. Zeigler	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The threats facing America today are different from the threats on 9/11. The actions the United States took to defend against similar attacks were necessary; however, the increase in attacks by non-foreign terrorist organizations (FTOs) requires agencies to evolve. This thesis explores how the Transportation Security Administration (TSA) can be leveraged to enhance the intelligence capabilities of the U.S. government. This thesis begins by identifying the threats facing America in 2021. Through a review of legislation, government sources, and scholarly work, this thesis presents the debate amongst sources on the threats America is facing and the role the U.S. government is taking to defeat the threats. This thesis lays out the TSA's current intelligence structure and the legislation in which the TSA operates against today's threats. Finally, this thesis provides the existing legal framework that allows the TSA to enhance its intelligence activity for U.S. national security. The findings reveal FTOs are no longer the number one threat. The research shows an increase in different threats to America, such as domestic terrorism, transnational organized crime, and espionage within the homeland. To confront these threats, the TSA must evolve to defend the U.S. transportation sector by enhancing its intelligence activity with the U.S. government. Further, this thesis shows current legislation provides a roadmap for the TSA to participate in additional intelligence activities.

14. SUBJECT TERMS intelligence, homeland security, Department of Homeland Security, DHS, Transportation Security Administration, TSA, intelligence community, inter-agency collaboration, information sharing, foreign terrorist organizations, FTO	**15. NUMBER OF PAGES** 107
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

LEVERAGING DHS ASSETS: POTENTIAL FOR THE TRANSPORTATION SECURITY ADMINISTRATION TO ENHANCE U.S. GOVERNMENT INTELLIGENCE CAPABILITIES

Zachary D. Zeigler
Intelligence Operations Officer, Transportation Security Administration
BA, Idaho State University, 2007

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
October 2021**

Approved by: Cristiana Matei
Co-Advisor

Paul J. Smith
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The threats facing America today are different from the threats on 9/11. The actions the United States took to defend against similar attacks were necessary; however, the increase in attacks by non-foreign terrorist organizations (FTOs) requires agencies to evolve. This thesis explores how the Transportation Security Administration (TSA) can be leveraged to enhance the intelligence capabilities of the U.S. government. This thesis begins by identifying the threats facing America in 2021. Through a review of legislation, government sources, and scholarly work, this thesis presents the debate amongst sources on the threats America is facing and the role the U.S. government is taking to defeat the threats. This thesis lays out the TSA's current intelligence structure and the legislation in which the TSA operates against today's threats. Finally, this thesis provides the existing legal framework that allows the TSA to enhance its intelligence activity for U.S. national security. The findings reveal FTOs are no longer the number one threat. The research shows an increase in different threats to America, such as domestic terrorism, transnational organized crime, and espionage within the homeland. To confront these threats, the TSA must evolve to defend the U.S. transportation sector by enhancing its intelligence activity with the U.S. government. Further, this thesis shows current legislation provides a roadmap for the TSA to participate in additional intelligence activities.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

9/11	September, 11, 2001 terrorist attacks
AAR	after action report
ACLU	American Civil Liberties Union
AQ	al-Qaeda
ATSA	Aviation and Transportation Security Act of 2001
AWD	Atomwaffen Division
CBP	Customs and Border Protection
CHDS	Center for Homeland Defense and Security
CIA	Central Intelligence Agency
CIP	component intelligence program
CMO	Collection Management Officer
CRS	Congressional Research Service
CSIS	Center for Strategic and International Studies
CT	counterterrorism
DCI	Director of Central Intelligence
DDI	Directorate of Digital Innovation
DEA	Drug Enforcement Administration
DHS I&A	DHS Office of Intelligence and Analysis
DHS IE	DHS Intelligence Enterprise
DHS OIG	DHS Office of Inspector General
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DNI	Director of National Intelligence
DOD	Department of Defense
EAB	Encounter Analysis Branch
EO 12333	Executive Order 12333
FAA ESSA	Federal Aviation Administration Extension, Safety, and Security Act
FAMS	Federal Air Marshal Service
FBI	Federal Bureau of Investigation

FIID	Field Intelligence Integration Division
FIO	Field Intelligence Officer
FTO	foreign terrorist organization
GAO	Government Accountability Office
HC	human capital
hDNA	human Deoxyribonucleic acid
HSIN	Homeland Security Information Network
HSIPF	Homeland Security Intelligence Priority Framework
HSPD-6	Homeland Security Presidential Directive 6
HUMINT	Human Intelligence
HVE	homegrown violent extremists
I&A	Intelligence & Analysis
IC	Intelligence Community
ICD 204	Intelligence Community Directive—204
ICD 900	Intelligence Community Directive—900
IIR	intelligence information report
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISIS	Islamic State of Iraq and Syria
IWW	Indications and Warning Watch
KST	known or suspected terrorist
LE	law enforcement
MOU	Memorandum of Understanding
N3AG	Nazi National Action Group
NCTC	National Counterterrorism Center
NIM	National Intelligence Manager
NIM-A	National Intelligence Manager—Aviation
NIP	National Intelligence Program
NIPF	National Intelligence Priorities Framework
NIS	National Intelligence Strategy
NPS	Naval Postgraduate School
NRM	Nordic Resistance Movement
NSA 47	National Security Act of 1947

NTVC	National Transportation Vetting Center
ODNI	Office of the Director of National Intelligence
QS	Quiet Skies
RTT	Revolt through Tradition
SLTT	state, local, tribal and territorial
SP	Silent Partner
STA	Security Threat Assessment
TAD	Transportation Analysis Division
TOC	transnational organized crime
TSA	Transportation Security Administration
TSA I&A	TSA Office of Intelligence Analysis
TSAR	TSA representatives
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database (consolidated watchlist)
TSOC	Transportation Security Operations Center
TVS	Transportation Vetting System
UDHSIC	Unifying DHS Intelligence Components Act
USCG	United States Coast Guard
USPER	United States person
VAD	Vetting Analysis Branch
WebEOC	web-based system
WTA	World Threat Assessment

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

After the September 11, 2001 terrorist attacks (9/11), the U.S. Intelligence Community (IC) and law enforcement (LE) agencies were re-structured to respond to the types of attacks encountered at that time. The changes occurred from a reactionary posture and were deemed necessary to ensure the safety of America moving forward.[1] However, the last 20 years has seen an increase in domestic terrorism, transnational organized criminal (TOC) activity, and espionage from bad actors resident in the homeland. This increase in activity has caused the U.S. IC and LE agencies to plan, budget, and reorganize their organizations to tackle these threats more effectively.

Within the Department of Homeland Security (DHS), refinement has resulted in multiple systems collecting vast amounts of information and analyzing the data, in part, for vetting and watchlisting purposes. This refinement also included the creation of the Transportation Security Administration (TSA). The TSA is ideally positioned to access valuable data, which can be of further use in the U.S. fight to counter threats to the homeland. This thesis argues that the TSA needs to enhance information sharing with U.S. government organizations through enhanced intelligence capabilities. The opportunity cost in failing to improve the TSA's intelligence collection is an overall loss of intelligence that can be usefully applied by multiple U.S. IC and LE agencies against the diverse threats America is currently facing.

To demonstrate the need for modernizing the TSA's intelligence functions, this thesis explores the unclassified literature on the threats facing America today and the IC's responsibilities since 9/11, as well as the TSA's support to intelligence. The TSA was created to secure the nation's public transportation sector, albeit with a focus on the screening of airline passengers. Almost two decades later, some still espouse overseas terrorism as the number one threat, such as former National Security Advisor John R.

[1] Robert S. Mueller, III, "The FBI Transformation since 2001," 1, Federal Bureau of Investigation, September 14, 2006, https://www.fbi.gov/news/testimony/the-fbi-transformation-since-2001.

Bolton (2018–2019) who proclaims "radical Islamist militants" are the highest threat facing America today.[2]

On the flip side, the research shows that the United States is no longer concerned with solely countering threats from overseas terrorist organizations akin to al-Qaeda and ISIS. In fact, Michael C. McGarrity, former Assistant Director of the Federal Bureau of Investigation's Counterterrorism Division (2018–2019), noted, "there have been more arrests and deaths caused by domestic terrorists than international terrorists in recent years."[3] Further, the 2019 *United States National Intelligence Strategy* puts a significant precedence on traditional state actors, such as Russia, China, Iran, and North Korea.

While overseas terrorism, domestic terrorism, and traditional threat actors are high priority targets for the U.S. government, the threat from TOCs poses just as much risk. A recent report by RAND presents the emergent threat of TOC actors as a "hybrid" that "combines aspects of criminal organizations, terrorist groups, and insurgencies," and believes TOCs "pose crosscutting threats to U.S. security interest."[4] Over the last seven years, according to the TSA's *Insider Threat Roadmap*, the TSA has encountered several incidents involving TOC actors, such as a 2018 event that busted several airline workers for smuggling illegal drugs, for a TOC group, onto departing aircraft.[5]

Along with the TOC and insider threat, the TSA is concerned that "terrorists could exploit the tactics, techniques, and procedures used by the transnational criminal

---

[2] Mark Landler and Eric Schmitt, "Terrorist Threat 'More Fluid and Complex than Ever,' White House Says," *New York Times*, sec. 1, United States, October 4, 2018, https://www.nytimes.com/2018/10/04/us/politics/trump-counterterrorism-strategy.html.

[3] Michael C. McGarrity and Calvin A. Shivers, "Confronting White Supremacy, Statement before the House Oversight and Reform Committee, Subcommittee on Civil Rights and Civil Liberties Washington, D.C.," 1, Federal Bureau of Investigation, June 4, 2019, https://www.fbi.gov/news/testimony/confronting-white-supremacy.

[4] Angel Rabasa et al., *Counternetwork: Countering the Expansion of Transnational Criminal Networks* (Santa Monica, CA: RAND, 2017), XVI, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1481/RAND_RR1481.pdf.

[5] David P. Pekoske, *Insider Threat Roadmap 2020* (Washington, DC: Transportation Security Administration, 2020), 6, https://www.tsa.gov/sites/default/files/3597_layout_insider_threat_roadmap_0424.pdf.

organizations" to recruit credentialed TSA insiders.[6] Defeating these shifting threats requires the TSA to transform just as the IC and the members within the IC have changed to confront the existing threats to the United States.[7]

For the TSA to support the IC's efforts, by enhancing the TSA's intelligence functions, fundamental changes need to be made within the organization. The TSA is aware change should occur.[8] However, current scholarship reveals that opinions are varied on the how the TSA should be employed. Former U.S. Representative John Mica (R-Fla) (1993–2017) stated that he would like to see the TSA hand over the screening business to private security companies and focus "on intelligence to identify and address threats."[9] Other research believes the TSA has gone too far in its intelligence activity to include the DHS Office of Inspector General findings on the Federal Air Marshal Service Quiet Skies program stating the "TSA did not properly plan, implement, and manage the Quiet Skies program to meet the program's mission of mitigating the threat to commercial aviation posed by higher risk passengers."[10] In light of the research, the TSA can transform itself, as some members of the IC have done, so that the TSA can better position itself for the future and provide enhanced intelligence capabilities to the U.S. government.

While the TSA is not a statutory member of the IC, the TSA is a member of the DHS intelligence enterprise (IE), and as such, supports the U.S. intelligence activities. This thesis found that the DHS Office of Intelligence and Analysis's (DHS I&A) statutory IC membership provided a pathway for the TSA to provide enhanced intelligence collection

---

6 Pekoske, 6.

7 James Burch, "The Domestic Intelligence Gap: Progress since 9/11?," *Homeland Security Affairs* XVII, 1, April 1, 2008, https://www.hsaj.org/articles/129.

8 Patricia F. S. Cogswell, "Protecting the Nation's Transportation Systems: Oversight of the Transportation Security Administration," Transportation Security Administration, 1, September 11, 2019, https://www.tsa.gov/news/press/testimony/2019/09/11/protecting-nations-transportation-systems-oversight-transportation.

9 Andrew Becker, "Lawmaker Says TSA Should Focus on Intelligence, Get out of Screening," National Security, Reveal from the Center for Investigative Reporting, para. 1, April 28, 2016, https://www.revealnews.org/blog/lawmaker-says-tsa-should-focus-on-intelligence-get-out-of-screening/.

10 Joseph V. Cuffari, *TSA Needs to Improve Management of the Quiet Skies Program (REDACTED)* (Washington, DC: Office of the Inspector General, Department of Homeland Security, 2020), 2, https://www.oig.dhs.gov/sites/default/files/assets/2020-11/OIG-21-11-Nov20-Redacted.pdf.

to contribute to improved IC analysis of potential threats to the United States' national security. Just as the DHS was established to be "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur," the TSA was established to act as a deterrent to future attacks through its operational and analytic activities.[11] The research identified the TSA's current intelligence structure and legal authorities in which it could operate. This thesis has laid out the legal framework to support any future intelligence enhancements.

Indeed, the existing laws and directives already address the issue of whether the U.S. government, specifically the IC, can legally support expanding the TSA's intelligence functions to answer national intelligence priority requirements.[12] These laws include the National Security Act of 1947 that clearly defines the components of the IC that include the DHS I&A. The DHS I&A oversees the DHS IE, of which the TSA is a member. Additionally, this thesis identified that Executive Order 12333 stipulated that to acquire insight on any threats toward the United States, the intelligence needed to be of the highest quality and been obtained through appropriate and legal means. The responsibility to analyze and disseminate intelligence falls on each department and agency within the IC.[13] Further stating that in coordination with relevant organizational leaders, the Director of National Intelligence (DNI) can seek the support of non-IC organizations to engage in the collection and analysis of intelligence pertinent to national security.[14]

This thesis found that the TSA was required to provide the DNI with the highest quality intelligence. Further, the research found that the Intelligence Community Directive—900 and Intelligence Community Directive—204 laid out the responsibility of

---

[11] George W. Bush, *National Strategy for Homeland Security* (Washington, DC: White House, 2002), 2, https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf.

[12] These authorities are derived from the TSA's current position within the DHS, as discussed in Chapter III, the Congressional mandates that established the TSA, and existing laws and directives in place that guide the IC's common framework.

[13] Ronald Reagan, Executive Order 12333, "United States Intelligence Activities," National Archives, 12, Part 3, General Provisions, December 4, 1981, https://www.archives.gov/federal-register/codification/executive-order/12333.html.

[14] Reagan.

the National Intelligence Manager of Aviation (NIM-A) to provide the DNI with all intelligence related to aviation. The NIM-A was also required to advise the DNI on the creation of national intelligence priorities, to include intelligence needs and intelligence gaps, as well as ad-hoc priorities for emergent intelligence needs, respectively.[15] The research found that these authorities allowed the TSA to participate in additional intelligence activities usually associated with statutory IC members. Through the NIM-A, the TSA could begin to establish national intelligence priorities that not only answered intelligence gaps in the U.S. transportation sector but also supported the larger IC requirements.

This research suggests that today's threats are more encompassing than foreign terrorist organizations, and that the TSA must evolve to respond to the emerging threats on the aviation ecosystem and the entire U.S. transportation sector. Further, this thesis found that the TSA was already providing occasional valuable intelligence to the IC and LE communities. The TSA nevertheless can provide more value to the IC through advanced intelligence collection, dissemination of raw intelligence, as well as preparing strategic analytic products. Finally, this thesis found that existing legislation would allow the TSA to participate legally in additional intelligence gathering activities in support of the U.S. IC.

The first recommendation is for the IC to develop specific transportation intelligence requirements that are unique to the TSA. With the creation and inclusion of transportation intelligence requirements, the TSA can then provide a definitive roadmap for intelligence activities.[16] The second recommendation is to establish a collection management program at the TSA. Collection management is used to interpret intelligence requirements into tactical or strategic operational objectives and directs those collecting

---

15 Director of National Intelligence, *Intelligence Community Directive 900—Integrated Mission Managemen*t (Washington, DC: Office of the Director of National Intelligence, 2013), https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives.

16 Todd Rosenblum, "Homeland Intelligence: The Unique Community within the Community," *The Cipher Brief* (blog), 1, October 9, 2016, https://www.thecipherbrief.com/column_article/homeland-intelligence-the-unique-community-within-the-community.

information and those analyzing the collected information.[17] The third recommendation is to modernize the TSA's intelligence functions. No organization can function at the highest level or provide a superior product if it is not continually improved. Finally, the fourth recommendation is to develop a TSA overt strategic debriefing program. Such a program would be responsible for developing and executing overt Human Intelligence collection operations. These operations would include intelligence debriefings of overt sources, drafting raw intelligence reports, responding to customer requests for intelligence and collection management requirements, as well as maintaining detailed operational records.

[17] George J. Franz, "Beyond Desert Storm—Conducting Intelligence Collection Management Operations in the Heavy Division" (monograph, Fort Leavenworth, KS, School of Advance Military Studies, United States Army Command and General Staff College, 1995), 8–13, https://apps.dtic.mil/dtic/tr/fulltext/u2/a309837.pdf.

ACKNOWLEDGMENTS

Several individuals contributed to the success of completing this thesis. First and foremost, I want to thank my wife, Karly. She has been my grounding force throughout this process and provided comfort when I thought I could not push through. I am thankful to all six of my children, who patiently waited outside my office doors to spend time with me.

I am extremely grateful to my advisors, Dr. Cristiana Matei, and Mr. Paul Smith, for their tremendous patience, excellent guidance, and encouraging comments along the way. The insights each of them provided from their extensive professional backgrounds paved the way in so many areas of this thesis. During those times where I thought I was providing the reader with clarity, both Cris and Paul graciously pointed me in the right direction.

Without the support of my senior leadership team, Skyler Dickinson, and Christina Chesterfield, I would not have been provided the time or agency resources to complete this work. I thank them and my other colleagues who provided input and suggestions along the way. Their experience and trail blazing efforts are exemplars of our future government leaders.

To each scholar and guest speaker at the Center for Homeland Defense and Security (CHDS), I will be continually amazed at your dedication and constant support to each student who passes through the Naval Postgraduate School (NPS) halls.

Finally, I am thankful for each member of the 1801/1802 NPS CHDS cadre for your help and encouragement to flush out my initial thesis ideas and create a product in such a supporting environment. I wish all of you continued professional and personal success.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

"So that's it," John E. McLaughlin, former Deputy Director of the Central Intelligence Agency (CIA) remembered thinking when the last airplane struck its target on September 11, 2001.[1] It was a moment in American history when the veil of homeland protection fell like a gauntlet. Foreign terrorists wielding box cutters and an understanding of some U.S. security gaps attacked the United States through the public transportation sector. By the end of that same day, Mr. McLaughlin stated what most Americans already felt, "nothing will ever be the same."[2]

So much of that statement is true for those who remember the 2001 attacks. From that point, and to defend from any further hostile activity on the homeland, the United States took aggressive military, investigative, and legislative actions to protect the security of its borders.[3] Included in those actions, the U.S. Congress created the Transportation Security Administration (TSA) and charged it with "security in all modes of transportation," a rather challenging task.[4]

Since its inception, the TSA has supported the mission to secure the public transportation infrastructure, albeit with most efforts concentrated on the aviation ecosystem.[5] The TSA's perspective has been focused on security and ensuring that terrorists are unable to highjack another commercial airliner to cause further damage on

---

[1] Dina Temple-Raston, "The State of Intelligence: Fifteen Years after 9/11," 1, Council on Foreign Relations, September 12, 2016, https://www.cfr.org/event/state-intelligence-fifteen-years-after-911.

[2] Temple-Raston.

[3] History.com Editors, "Reaction to 9/11," History, August 7, 2019, https://www.history.com/topics/21st-century/reaction-to-9-11.

[4] Aviation and Transportation Security Act of 2001, *U.S. Code* 51 (2001): 1 § 101, 115 et seq., https://www.congress.gov/bill/107th-congress/senate-bill/1447.

[5] The term "aviation ecosystem" refines the term "aviation domain" and is intended to include all aspects of airports, airlines, aircraft, airlift, actors, and aviation management. This term is a more holistic, robust description of the reality of modern aviation and more fully captures the global scope and complexity of the industry and the economic impact it generates. The term underscores the vast, interconnected systems that comprise domestic and international aviation, including civil (both commercial and general) and public aviation. Donald J. Trump, *National Strategy for Aviation Security of the United States of America* (Washington, DC: White House, 2018), 17–18, https://www.hsdl.org/?abstract&did=821736.

U.S. soil. However, in the last 20 years, "a complex threat landscape with enemies and adversaries who are constantly evolving," has emerged as a threat against the nation.[6] These adversaries include overseas terrorist organizations, such as al-Qaeda (AQ) and the Islamic State of Iraq and Syria (ISIS), U.S.-based far-right hate groups like the Proud Boys, and Transnational Organized Criminals. These groups and organizations have attempted to disrupt, penetrate, or use the transportation sector for nefarious purposes. As an example, in 2018, a group of U.S. aviation workers were arrested after being caught using their TSA credentials to access and bypass airport security measures. This group was thus able to smuggle drugs onto departing passenger aircraft.[7] As such, the United States and the legal, investigative, and intelligence systems in place to defeat threats against the nation should continue to evolve as well.

Indeed, the new rising concerns go beyond countering terrorism threats that mimic the atrocities of the September 11, 2001 terrorist attack (9/11). To remain consistent with the DHS guiding principles to "remain resolute against today's threats and hazards by keeping pace with our adversaries," it will be valuable to incorporate the TSA's existing domestic and international footprint to develop its capabilities further as an intelligence provider.[8] Such an investment will expand the U.S. government's counterterrorism knowledge base and better protect American citizens.

A. THREATS TO THE UNITED STATES

In the 2019 National Intelligence Strategy (NIS), the Office of the Director of National Intelligence (ODNI) summarizes the hostile environment the United States faces as progressively more intricate and ambiguous in which threats are increasingly varied and

---

[6] Kevin K. McAleenan, *The DHS Strategic Plan Fiscal Years 2020–2024* (Washington, DC: Department of Homeland Security, 2019), I, https://www.dhs.gov/publication/department-homeland-securitys-strategic-plan-fiscal-years-2020-2024.

[7] David P. Pekoske, *Insider Threat Roadmap 2020* (Washington, DC: Transportation Security Administration, 2020), 6, https://www.tsa.gov/sites/default/files/3597_layout_insider_threat_roadmap_0424.pdf.

[8] McAleenan, *DHS Strategic Plan*, 3.

interrelated.[9] In addition to the internal and external terrorism threats from foreign terrorist organizations (FTOs), the ODNI is concerned with transnational crimes and the insider threat. The ODNI NIS report claims that foreign intelligence entities actively seek out ways to further their ideological beliefs—using cyber tools, malicious insiders, espionage, and supply chain exploitation—to penetrate and disrupt the interests of the United States.[10] This section reviews the priority threats to U.S. national security.

1. Terrorism Threat from Overseas

Since 9/11, the United States has spent large sums of money to protect its borders from further attacks.[11] It appears that there has been a great deal of success on this front. No further large-scale terrorist activities have occurred within the U.S. aviation ecosystem.[12] Much of this protection has been accomplished through the creation and expansion of multiple government agencies, as well as investment in traditional law enforcement (LE) and intelligence collection, analysis, and dissemination.[13] The terrorism threats from overseas are ever present and require continued attention.

The United States faces the threat of terrorism sponsored by nation states including, for example, Iran that supports militant and terrorist groups throughout the world, such as the Lebanese Hizballah (Hizballah).[14] Through the Islamic Revolutionary Guard Corps, Qods Force, Iran provides groups like Hizballah with money, training, and operational

---

[9] Daniel R. Coats, *National Intelligence Strategy of the United States of America* (Washington, DC: Office of the Director of National Intelligence, 2019), 4, https://www.dni.gov/index.php/newsroom/reports-publications/item/1943-2019-national-intelligence-strategy.

[10] Coats, 14.

[11] Neta C. Crawford, *Costs of War* (Providence, RI: Brown University, Watson Institute International and Public Affairs, 2018), 2–6, https://watson.brown.edu/costsofwar/files/cow/imce/papers/2018/Crawford_Costs%20of%20War%20Estimates%20Through%20FY2019%20.pdf.

[12] Erik Goepner and Trevor A. Thrall, "Time to Step Back from the War on Terror," Cato Institute, October 26, 2017, https://www.cato.org/publications/commentary/time-step-back-war-terror.

[13] David Inserra, "Here's How Safe We Are 17 Years after 9/11," 1, The Heritage Foundation, September 11, 2018, https://www.heritage.org/homeland-security/commentary/heres-how-safe-we-are-17-years-after-911.

[14] Nathan A. Sales, "Countering Iran's Global Terrorism," Department of State, November 13, 2018, https://www.state.gov/countering-irans-global-terrorism/.

direction. Due to Iran's sponsorship of terrorism, Hizballah maintains an extensive military and intelligence capability, stockpiles modern arms, and retains a widespread network of operatives and sympathizers overseas to include individuals located within the United States.[15] These threat actors seek to interrupt American democracy through traditional forms of violent terrorism, as well as leveraging emerging technology including "the emergence of more secure modes of communications, the expansion of social and mass media, and persistent instability across several regions."[16]

According to the *National Strategy for Counterterrorism*, not only is the United States concerned with nation state actors and groups like AQ and ISIS, it is also worried about revolutionary, nationalist, and separatist movements, such as the Nordic Resistance Movement (NRM), the neo-Nazi National Action Group (N3AG), and Babbar Khalsa International.[17] These organizations use violence and assassinations to disrupt political parties, economic interests, and religious organizations. While these movements have not committed terrorist activities within the homeland, sans AQ, their terrorist actions place U.S. citizens and foreign interests at risk, especially Americans and American businesses operating overseas.[18] Additionally, the NRM and N3AG have interacted and shared their anti-western views with organizations inside the United States. Each of these organizations is determined to impose its will against America by influencing and recruiting like-minded individuals to engage in terroristic behavior.

As opposed to 2001, the planning, prepping, and executing of an attack can be accomplished in relative anonymity online and can be accomplished in less time across multiple borders. To combat these types of enemies, the United States must remain agile in its approach to countering these threats and be creative in the way it uses agencies to pursue these terrorists.

---

[15] Donald J. Trump, *National Strategy for Counterterrorism of the United States of America* (Washington, DC: White House, 2018), 9–10, https://www.dni.gov/files/NCTC/documents/news_documents/NSCT.pdf.

[16] Trump, 7–10.

[17] Trump, 9.

[18] Trump, 11.

2. The Threat from Domestic Terrorism

While preventing threats from foreign entities remains a top priority for the U.S. government, domestic terrorism is also on the rise.[19] Over the last six years, a significant spike in violent domestic terrorist activity has resulted because recruitment and radicalization has become quicker and easier through online forums.[20] According to the Center for Strategic and International Studies (CSIS), hundreds of terrorist plans or attacks have occurred in the United States since 2015.[21] The challenge for the U.S. IC and LE community is to mine the suspects of these plans and attacks showing signs of radicalization or terrorist affiliation.

In December 2015, two U.S. citizens inspired by the foreign terrorist group ISIS, opened fire inside the training room of the San Bernardino Environmental Health Services Department and killed 14 people.[22] Both assailants, Syed Farook and his wife Tashfeen Malik, were able to flee the scene and continue to wreak havoc when later confronted by the police. They began to open gunfire on the police officers until the suspects were finally shot dead.[23] Then, in June 2016, Omar Mateen, who also swore allegiance to ISIS, opened gunfire inside a Florida nightclub killing 49 people. The nightclub attack was the deadliest terrorist attack in America since the 2001 attacks. In both incidents, authorities at the local, state, and federal level were unaware of the suspects' affiliation or plans. While these two incidents were conducted under the guise of religious terrorism, far-right extremists, and

---

[19] Legally classifying domestic terrorism appears to be a challenge for authorities. The difficultly in distinguishing between a domestic terrorist and a person committing a violent crime is based on the definition. Domestic terrorism in the United States is defined as "ideologically motivated acts that are harmful to human life and intended to intimidate civilians, influence policy, or change government conduct." Trevor Aaronson, "Terrorism's Double Standard: Violent Far-Right Extremists Are Rarely Prosecuted as Terrorists," 1, The Intercept, March 23, 2019, https://theintercept.com/2019/03/23/domestic-terrorism-fbi-prosecutions/.

[20] Michael C. McGarrity, "Confronting the Rise of Domestic Terrorism in the Homeland," 1, Federal Bureau of Investigation, May 8, 2019, https://www.fbi.gov/news/testimony/confronting-the-rise-of-domestic-terrorism-in-the-homeland.

[21] Seth G. Jones, Catrina Doxsee, and Nicholas Harrington, *The Escalating Terrorism Problem in the United States* (Washington, DC: Center for Strategic & International Studies, 2020), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200612_Jones_DomesticTerrorism_v6.pdf.

[22] Jeremiah J. Hart, "Strategic Mutual Aid Response to Terrorism: A New Approach" (master's thesis, Naval Postgraduate School, 2020), 25, https://www.hsdl.org/?abstract&did=839423.

[23] Hart, 26–34.

particularly members associated with white supremacy and militias, plan and execute most of the domestic terrorist attacks in the United States.[24]

Over the last two years, members who affiliate with far-right organizations have conducted numerous attacks that have been violent, deadly, and have stoked fear into the hearts and minds of the American public. According to a report by the United Nations, the COVID-19 pandemic may have contributed to the increase in domestic terrorism in the United States by providing plenty of time for vulnerable people to view extremist propaganda online and engage with like-minded individuals. This contact has led them to radicalize, which in some cases, has also led them to engage in violence.[25] Throughout 2020, right-wing terrorists conducted and carried out seven high-profile terrorist acts. In October 2020, the Federal Bureau of Investigation (FBI) arrested 13 individuals who were preparing to kidnap the governor of Michigan because they believed that the governor's policies to limit the spread of COVID-19 were illegal. All the individuals involved were affiliated with the Boogaloo movement.[26] Domestic terrorism is directly impacting the TSA and how it approaches the vetting and analysis of the people affiliated with the U.S. transportation sector.

The most recent and highly visible and reported domestic terrorist attack occurred in January 2021 during the certification of the Presidential Electoral College vote by the U.S. Congress. Pro-Trump supporters overran the security perimeter of the U.S. Capitol building and forced entry into the government facility. The panic and fear of that incident was broadcast worldwide, with most people in shock and fear of the potential outcome.

---

[24] Dan Glaun, "A Timeline of Domestic Extremism in the U.S., from Charlottesville to January 6," Public Broadcasting Service, Frontline, April 21, 2021, https://www.pbs.org/wgbh/frontline/article/timeline-us-domestic-extremism-charlottesville-january-6/.

[25] Antonia Marie De Meo, *Stop the Virus of Disinformation: The Risk of Malicious Use of Social Media during COVID-19 and the Technology Options to Fight It* (Turin, Italy: United Nations Interregional Crime and Justice Research Institute (UNICRI), 2020), 7–9, http://www.unicri.it/sites/default/files/2020-11/SM%20misuse.pdf.

[26] The Boogaloo movement, whose cohorts are often referred to as "Boogaloo Boys" or "Boogaloo Bois," is a developing "anti-government extremist movement that formed in 2019. In 2020, boogaloorers increasingly engaged in real world activities as well as online activities, showing up at protests and rallies around gun rights, pandemic restrictions and police-related killings." The term "boogaloo" is in reference to a future civil war. "The Boogaloo Movement," Anti-Defamation League, accessed June 14, 2021, https://www.adl.org/boogaloo.

Sadly, five people died during that attack. According to the George Washington University Program on Extremism Project, 569 people and counting have been arrested and charged with various crimes due to their involvement with the Capitol terrorist act.[27] When reviewing the criminal complaints and indictments on these individuals, some of the people charged have a nexus to the U.S. transportation sector who include truck drivers, pilots, and even state police forces.[28] Individuals who display such derogatory action against the nation are a threat to the transportation system from the inside.

Identifying individuals within the homeland who maintain or are developing violent ideological tendencies can be difficult. However, some of these individuals appear to have access to sensitive information and facilities, such as the aviation worker who is intimate with airport security protocols and can attack with little to no warning. To protect these assets, the U.S. government must continually look for ways to improve its overall collection and dissemination of valuable threat information. Taking advantage of the organizations, strategies, and policies in-place will provide greater coverage and identification of individuals with nefarious agendas. In a response to the ODNI's 2021 assessment on domestic violent extremism in the United States, President Biden's administration has begun discussing ways in which agencies created to fight the international war on terrorism can be used to fight domestic terrorism.[29] The TSA's access to thousands of individuals who work in and around sensitive transportation environments, such as airports and cargo facilities, domestically and overseas, can be used to identify and report on those who seek to do harm to America.

---

[27] "Capitol Hill Siege," GW Program on Extremism, 2021, https://extremism.gwu.edu/Capitol-Hill-Cases. Citation is an Excel document located in the middle of the webpage.

[28] GW Program on Extremism. Citation is links associated with each identified individual.

[29] Betsy Woodruff Swan, "DHS Looking at Tracking Travel of Domestic Extremists," POLITICO, 1, March 23, 2021, https://www.politico.com/news/2021/03/23/homeland-security-domestic-extremists-477658; Director of National Intelligence, *(U) Domestic Violent Extremism Poses Heightened Threat in 2021* (Washington, DC: Office of the Director of National Intelligence, 2021), https://www.dni.gov/files/ODNI/documents/assessments/UnclassSummaryofDVEAssessment-17MAR21.pdf.

3. The Threat from Transnational Organized Crime

In his July 2019 comments to the Senate Judiciary Committee, Christopher Wray, Director of the FBI, stressed that today's transnational organized crime (TOC) enterprises represented a considerable and escalating threat to the security of the United States and its international partners.[30] The TOC networks endanger the security of legitimate governments through illicit activities of "stock market fraud and manipulation, cyber-facilitated bank fraud and embezzlement, drug trafficking, identity theft, human trafficking, money laundering, alien smuggling, public corruption, weapons trafficking, extortion, kidnapping, and other illegal activities."[31]

A major threat of transnational crime to national security, if left unchecked, is that most TOC groups wield extensive power and have deep financial pockets that can be used to influence state-backed economies and affect legitimate governments by corrupting public officials.[32] This type of social transition, as an effect of transnational crime, can be seen in places, such as Lebanon, Guatemala, Honduras, El Salvador, as well as West Africa and the Sahel.[33] Within these environments, nefarious organized groups have taken over certain amounts of responsibility from the legitimate governments, due to the TOC syndicates' willingness to employ violence and engage in bribery, coercion, and corruption.[34] Limiting the opportunities for these threats to take hold, and defeating the transnational criminal actors in place, requires a robust strategy and maximizing the assets at the disposal of the U.S. government.

---

[30] Christopher Wray, "Oversight of the Federal Bureau of Investigation," Federal Bureau of Investigation, heading Transnational Organized Crime (TOC) and Opioids, July 23, 2019, https://www.fbi.gov/news/testimony/oversight-of-the-federal-bureau-of-investigation-072319.

[31] Wray, para. 1.

[32] "What We Investigate: Transnational Organized Crime," Federal Bureau of Investigation, accessed April 25, 2019, https://www.fbi.gov/investigate/organized-crime.

[33] Angel Rabasa et al., *Counternetwork Countering the Expansion of Transnational Criminal Networks* (Santa Monica, CA: RAND, 2017), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1481/RAND_RR1481.pdf.

[34] National Security Staff, *Transnational Organized Crime: A Growing Threat to National and International Security* (Washington, DC: White House, 2011), 158, https://obamawhitehouse.archives.gov/node/60577.

The TSA is not immune from TOC networks. The U.S. transportation sector is used extensively in TOC activity, such as money laundering, people smuggling, weapons, and drug trafficking. In 2017, a former TSA security officer was sentenced to serve time in prison for actively supporting TOC smuggling operations for two years. As a federal employee within the aviation sector, the TSA officer wittingly provided sensitive information, on multiple occasions, to TOC members seeking to transport illegal drugs through U.S. airports. In this case, the TSA officer allowed TOC members to circumvent security screening of their baggage by informing the TOCs in which security lane the officer would be positioned to allow the TOCs' baggage to pass without additional screening.[35] This incident is not isolated. The TOC actors in this example could have easily been smuggling weapons or explosives that could have caused immediate and serious harm within an airport or onboard an airliner.

In referring to the *2011 Strategy to Combat Transnational Organized Crime*, the ODNI made clear the priority to develop, stabilize, and incorporate instruments of American power to combat transnational organized crime.[36] The ODNI believes this priority can be accomplished through additional intelligence collection and intelligence sharing by creating an environment of collaboration amongst U.S. authorities and foreign liaisons.[37]

4. The Threat from Espionage

Counterintelligence, insider threats, and whistleblowers, which typically fall under the espionage umbrella, carry with them significant risk to the homeland and national security of the United States. According to the International Spy Museum in Washington,

---

[35] "Former TSA Transportation Security Officer Sentenced to 21 Months in Prison for Circumventing Security Checkpoint Screening," 1, The United States Attorney's Office Northern District of California, United States Department of Justice, accessed May 24, 2021, https://www.justice.gov/usao-ndca/pr/former-tsa-transportation-security-officer-sentenced-21-months-prison-circumventing.

[36] "Transnational Organized Crime," 1, Office of the Director of National Intelligence, June 2011, https://www.dni.gov/index.php/who-we-are/organizations/ise/archive/additional-resources/2146-transnational-organized-crime.

[37] Office of the Director of National Intelligence, 1.

DC, over 10,000 spies are in the District of Columbia and the surrounding areas.[38] Traditionally, these spies, also referred to as intelligence officers, maintain a cover, such as diplomat, attaché or liaison, student, or simply an ordinary citizen.[39] All these individuals pose a potential threat to national security due to their professional objectives to gain access to non-public information and facilities. To gain access, these spies seek out well-placed individuals who are vulnerable to being recruited.[40] Eliminating all the vulnerabilities an individual presents is not possible. However, it is possible to identify and mitigate threats through advanced warning and reporting.

To be sure, one of the risks, under the espionage umbrella, is the loss of sensitive data that may ultimately lead to grave danger.[41] In December 2020, it was discovered that Russia had successfully infiltrated the network monitoring and management tools of the U.S. company SolarWinds.[42] The effects of this cyberattack are projected to leave tens of thousands of its customers vulnerable to an attack, as well as compromising the security of hundreds of public companies and U.S. federal government agencies.[43] Another risk, especially considering the insider threat, is the witting or unwitting personnel who have access to sensitive facilities, such as the sterile area of an airport, and can use their trusted positions for nefarious purposes.[44] For example, in 2017, the U.S. Justice Department

---

[38] J. J. Green, "City of Secrets: Estimated 10,000 People in DC Are Spies," 1, WTOP, June 17, 2019, https://wtop.com/j-j-green-national/2019/06/city-of-secrets-an-estimated-10000-dc-residents-are-spies-heres-how-they-blend-in/.

[39] C. D. Edbrook, "Principles of Deep Cover," *Studies in Intelligence* 5, no. Summer (1961): 31.

[40] Ursula M. Wilder, "The Psychology of Espionage, Why Spy?," *Studies in Intelligence* 61, no. 2 (June 2017): 18.

[41] National Counterintelligence Executive, *(U) U.S. Insider Threat Security Classification Guide 2013*, Version 1 (Washington, DC: Office of the Director of National Intelligence, 2013), 14, 18, https://www.dni.gov/files/documents/FOIA/DF-2016-00161.pdf.

[42] Christian T. Fjeld, "Hearings on the SolarWinds Hack and Possible Policy Responses," 1, Insights Center, Mintz, February 23, 2021, https://www.mintz.com/insights-center/viewpoints/2236/2021-03-04-hearings-solarwinds-hack-and-possible-policy-responses.

[43] Fjeld, 1.

[44] "The 'sterile area' refers to portions of an airport defined in the airport security program that provides passengers access to boarding aircraft and to which the access generally is controlled by the TSA, an aircraft operator, or a foreign air carrier." Lisa S. Dean, *Security Threat Assessment for SIDA and Sterile Area Workers* (Washington, DC: Transportation Security Administration, 2004), 2, https://www.dhs.gov/sites/default/files/publications/privacy_pia_sida_sw_0.pdf.

indicted a dozen TSA and airport employees for being insider threats, who at the behest of unknown influence actors, used their positions of trust and access to sensitive areas of the aviation ecosystem to support and engage in nefarious activity.[45]

While it is not possible to eliminate all threats, it is possible to reduce the probability of an attack. The human element is often the weakest link and offers the most risk in sensitive environments.[46] As such, it is imperative to have a baseline understanding of the people who have authorized access. In many cases, this type of information can be collected in a routine manner. Some investigations however may require expanding the TSA's current intelligence capabilities through organizational optimization, a defined collection management program with fully developed transportation intelligence priorities that align with national strategy, and an overt collection program that can collect threat information for maximum dissemination to the IC.

To combat these protean security threats, it is necessary to consider new approaches in terms of intelligence organizations, processes, and culture.[47]

B. PROBLEM STATEMENT

While U.S. IC and LE agencies have been re-structured since 9/11 to respond to the types of attacks encountered at that time, these changes occurred from a reactionary posture and were deemed necessary to ensure the safety of America moving forward.[48] In spite of these defensive measures, and per the *2019 National Strategy for Aviation*, terrorist groups still find the aviation ecosystem an appealing operational target.[49] For example, in

---

[45] District of Puerto Rico, U.S. Attorney's Office, "Twelve Current and Former TSA and Airport Employees Indicted for Smuggling Approximately 20 Tons of Cocaine," 1, Department of Justice, February 13, 2017, https://www.justice.gov/usao-pr/pr/twelve-current-and-former-tsa-and-airport-employees-indicted-smuggling-approximatley-20.

[46] Frank L. Greitzer et al., "Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis," *Indiana University Press E-Service Journal* 9, no. 1 (Fall 2013): 106–138.

[47] Laicie Heeley et al., *Counterterrorism Spending: Protecting America while Promoting Efficiencies and Accountability* (Washington, DC: Henry L. Stimson Center, 2018), 28, https://www.hsdl.org/?abstract&did=810501.

[48] Robert S. Mueller, III, "The FBI Transformation since 2001," Federal Bureau of Investigation, September 14, 2006, https://www.fbi.gov/news/testimony/the-fbi-transformation-since-2001.

[49] Trump, *National Strategy for Aviation Security*, 2.

December 2020, Cholo Abdi Abdullah was indicted as an operative of the overseas terrorist organization al Shabaab who was seeking to hijack an aircraft to carry out a September 11-style attack.[50] The aviation ecosystem provides terrorists a stage to inflict pain and death to the most people possible and with the publicity terrorists pursue.[51] Appreciatively, the policies and procedures to thwart these types of attacks have been refined to greatly limit threats towards the United States.[52] However, the last 20 years has seen an increase in domestic terrorism, transnational organized criminal activity, and espionage from bad actors resident in the homeland. This increase in activity has caused the U.S. IC and LE agencies to plan, budget, and reorganize their organizations to tackle these threats more effectively.[53]

Within the DHS, refinement has advanced using multiple systems to collect vast amounts of information and then to analyze the data, in part, for vetting and watchlisting purposes.[54] This type of work by the DHS, in collaboration with the IC, has shown to be effective in reducing the threats from outside U.S. borders.[55] Recognizing the DHS's effectiveness against threats, and given the enormous U.S. intelligence and security apparatus, consideration should be given to leverage the DHS's collection of systems, policies, and procedures further to counter today's more complex threats more fully.[56] In doing so, the U.S. government needs to look no further than the components that make up the DHS and its intelligence capabilities. The components' intelligence units are daily

---

[50] "Kenyan National Indicted for Conspiring to Hijack Aircraft on Behalf of the Al Qaeda-Affiliated Terrorist Organization Al Shabaab," Office of Public Affairs, December 16, 2020, https://www.justice.gov/opa/pr/kenyan-national-indicted-conspiring-hijack-aircraft-behalf-al-qaeda-affiliated-terrorist.

[51] Trump, *National Strategy for Aviation Security*, 3.

[52] Goepner and Thrall, "Time to Step Back."

[53] Heeley et al., *Counterterrorism Spending*, 28.

[54] Donald J. Trump, *National Security Presidential Memorandum-9* (Washington, DC: White House, 2018), 4, https://www.dhs.gov/sites/default/files/publications/NSPM-9%20Implementation%20Plan.pdf.

[55] John F. Kelly, "Home and Away: DHS and the Threats to America," Department of Homeland Security, April 18, 2017, https://www.dhs.gov/news/2017/04/18/home-and-away-dhs-and-threats-america.

[56] Dana Priest and William M. Arkin, "The Secrets Next Door," *Washington Post*, sec. Investigative, July 21, 2010, https://www.washingtonpost.com/investigations/top-secret-america/2010/07/21/secrets-next-door/.

encountering all the threat streams described previously. Value can be further exploited through additional collection platforms, refined analysis, and standardized dissemination to the IC. One of those components is the TSA.

The TSA is ideally positioned to access valuable data, which can be of further use in the U.S. fight to counter threats to the homeland. Currently, the U.S. government, specifically the IC, may not be taking full advantage of the information collected. Further, additional avenues for intelligence collection, analysis, and dissemination are available. The TSA can contribute to these additional avenues. In talking about today's current mission space and leveraging all available assets, former CIA Director Gina Haspel (2018–2021) stated, "a bigger footprint…can get more done where it really counts."[57] This footprint not only applies to foreign partner liaisons, but also to further collaboration between U.S. government entities within the U.S. IC.

The assets at the disposal of the U.S. government include the TSA's daily encounters with multiple known or suspected terrorists (KSTs), the daily vetting of over 20 million credentialed transportation employees and over two million airline passengers, as well as the continual engagement with foreign entities and international transportation stakeholders.[58] These encounters provide the U.S. government one of the very few opportunities to be face-to-face with KSTs. During these events, the TSA can confirm or refute individuals' identities and their KST status, as well as garner additional intelligence data points that may expand on the knowledge of these individuals.

Additionally, the TSA conducts foreign airport assessments, air carrier inspections, and audits at foreign repair stations, which can be opportunities to provide valuable insights

[57] Gina Haspel, "CIA Director Gina Haspel Speaks at Auburn University," para. 29, Central Intelligence Agency, April 18, 2019, https://www.cia.gov/stories/story/cia-director-gina-haspel-speaks-at-auburn-university/.

[58] "Secretary Nielsen Receives Operational Briefing on Israeli Security Technology, Delivers Remarks at the International Homeland Security Forum," Department of Homeland Security, June 12, 2018, https://www.dhs.gov/news/2018/06/12/secretary-nielsen-receives-operational-briefing-israeli-security-technology-delivers.

about national intelligence priorities.[59] By the nature of such interactions, these previously noted insights allow the TSA the ability to peer inside the personnel and operational functions of foreign entities. In doing so, the TSA may determine its credibility and value as international partners and hold them accountable to help protect the aviation ecosystem.[60]

All these stated opportunities place the TSA in an advantageous position to collect a myriad of data on multiple events, whether through personal observation, technological means, or overt debriefings of DHS personnel and foreign partners. These opportunities could potentially enhance the IC's analytic capabilities if properly collected and reported.

However, due to interagency and bureaucratic reasons, the TSA's valuable intelligence opportunities have not been fully implemented. One example was the May 2021 cyberattack on the Colonial Pipeline, which led to confusion amongst U.S. government agencies and private industry partners.[61] Additionally, legal ambiguity seems to occur over how aggressively the TSA can collect and disseminate intelligence.[62] The IC moreover may not recognize the TSA's full capabilities since it is primarily viewed as a security agency confined to U.S. airports. Such an interpretation of the TSA has minimized

---

[59] *Examining TSA's Global Efforts to Protect the Homeland from Aviation Threats and Enhance Security at Last-Point-of-Departure Airports: Hearing before the Subcommittee on Transportation Security of the Committee on Homeland Security*, House of Representatives, 114th Cong., 1st sess., December 8, 2015, 3, https://www.hsdl.org/?abstract&did=806622.

[60] Jennifer Grover and Jessica Farb, *Aviation Security TSA Strengthened Foreign Airport Assessments and Air Carrier Inspections, but Could Improve Analysis to Better Address Deficiencies*, GAO-18-178 (Washington, DC: Government Accountability Office, 2017), https://www.gao.gov/assets/690/688730.pdf.

[61] The TSA spreads its intelligence functions over multiple divisions and offices. While communication occurs between these units, there appears to be different internal positions on what efforts can or should be implemented to carry out intelligence activities. These differences include the TSA's global strategies concerns of lost access to information should an unauthorized leak occur, the Field Intelligence Integration Division not having had an opportunity to expand the use of its deployed field intelligence officers' collection and reporting capabilities, and the TSA's intelligence analysis unit hidden away in vetting operations and, most striking, not exploiting the legal authorities available.

[62] The TSA is a derivative member of the IC by way of the DHS Intelligence and Analysis Division's statutory membership in the community. The TSA, along with seven other DHS components, have intelligence units that comprise the IE. However, the IE has not been thoroughly documented, nor have the IE authorities been fully recognized within the DHS, let alone the IC, to allow senior TSA leadership the clarity to carry out mandated intelligence functions. Mark A. Randol, *Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress*, CRS Report No. R40602 (Washington, DC: Congressional Research Service, 2010), 3–4, https://www.hsdl.org/?abstract&did=27362.

its potential long-term contribution to transportation intelligence and may be limiting opportunities to mitigate or defeat ongoing threats.

Consequently, this thesis argues that the TSA needs to enhance information sharing with the IC to mitigate threats to the United States. To enrich the partnership further between the TSA and U.S. IC, the IC should leverage the TSA's position and access to valuable information and explore new collection opportunities. Indeed, the information the TSA currently collects provides an opportunity to add to the overall threat knowledge base. At this point, the opportunity cost in failing to improve the TSA's intelligence collection is an overall loss of intelligence that can possibly be usefully applied by multiple U.S. IC and LE agencies against the diverse threats America is currently facing.

To illustrate the IC's available opportunity to increase its footprint by way of the TSA, this thesis explores the existing legal authorities and policies that can justify the expansion of the TSA's support to intelligence. While current legislation is not definitive regarding the TSA's ability to further its intelligence functions, the framework to justify any expansion is provided. This thesis aspires to identify how the IC can benefit and gain an advantage in its fight against ongoing threats by leveraging the TSA's position and access to information through legal authorities that formally recognize transportation intelligence, defined collection management, appropriate staffing alignment, advanced training, and the establishment of a debriefing program.

C. RESEARCH QUESTION

How can the U.S. IC better leverage the TSA's position and access to valuable information to enhance its efforts against ongoing threats to U.S. national security?

D. RESEARCH DESIGN

This thesis began with a reflection of the attacks on the United States in 2001 and the creation of the TSA, followed by the threats to the United States. From there, this thesis explored the unclassified literature on the threats facing America today and the IC's responsibilities since 9/11, as well as the TSA's intelligence support. Next, this thesis looked at the detailed role of TSA's intelligence operations, how this role would fit into

the DHS and the IC, and discussed the TSA's operating authorities. After that, the thesis examined existing legislation and policies to guide intelligence activity, and the TSA's possible use of the legislation and policies in its intelligence functions. Finally, the thesis presented recommendations to guide the TSA in moving forward with enhanced intelligence capabilities.

This thesis relied on primary sources, such as legislation, official government documents, and hearings related to the IC and the TSA. Secondary sources, such as books, academic journal articles, and reports, including Congressional Research Service (CRS) reports, documentaries, theses, and newspaper articles were also used.

E. THESIS OUTLINE

Chapter II provides a literature review of scholars debating the threats facing America today, the role the U.S. IC is playing to defeat the threats and the TSA's current role in intelligence. Then, Chapter III presents the TSA's current operations and the legislation under which it operates. Chapter IV provides the legal framework that justifies any enhanced intelligence efforts by the TSA to support the national intelligence cycle.[63] Finally, Chapter V provides findings, recommendations to enhance the TSA's support to intelligence, and then a conclusion, as well as proposals and recommendations for future research.

[63] The national intelligence cycle includes the planning and direction (requirements), collection of raw information, processing, analysis, and dissemination of finished intelligence products. The national intelligence cycle is repeated as policy and decision makers questions are answered, and then disseminated analysis ultimately invokes new questions from intelligence customers and policy makers.

II. LITERATURE REVIEW

This literature review presents scholarly works that discuss the threats facing America. This literature review also discusses different authors and scholars' opinions on the IC's role and changes since 9/11. Finally, this chapter provides a review of the literature that discusses the TSA's current support to intelligence.

A. THREATS TO THE UNITED STATES

Following al-Qaeda's use of commercial airplanes to attack America in 2001, the U.S. government began the process of building and restructuring its IC and LE agencies. This process intended to eliminate the chance for a repeat attack in the same vein. One of the steps in this process was the creation of the TSA. The TSA was created specifically to secure the nation's transportation network, with an emphasis on the screening of airline passengers. The literature review on the threats facing America follows.

As an investigative response to the September 2001 attacks, the U.S. government established the National Commission on Terrorist Attacks upon the United States (The Commission) to investigate and present the findings surrounding the September 11 attacks.[64] The Commission reported the U.S. government viewed overseas terrorist organizations as the number one threat to U.S. national security. Specifically, the Commission stated the U.S. government was concerned with "the threat posed by Islamist terrorism-especially the al Qaeda network, its affiliates, and its ideology."[65] At that time, most pundits, journalists, and authors agreed that the overseas terrorist threat was the top priority.

Almost two decades later, some still espouse overseas terrorism as the number one threat. The *2018 National Strategy for Counterterrorism* states, "radical Islamist terrorist remain the primary transnational terrorist threat to the United States and its vital

64 National Commission on Terrorist Attacks, *The 9/11 Commission Report* (Washington, DC: National Commission on Terrorist Attacks, 2004), https://govinfo.library.unt.edu/911/report/911Report.pdf.

65 National Commission on Terrorist Attacks, 362.

interests."[66] Even further, former National Security Advisor John R. Bolton (2018–2019), proclaimed the terrorism "landscape [is] more fluid and complex than ever" and stated "radical Islamist militants" to be the greatest threat facing America today.[67] In January 2019, when addressing members of the U.S. Senate, former DNI Dan Coats (2017–2019) informed lawmakers "terrorism remains a persistent threat and in some ways is positioned to increase."[68] Going further, Mr. Coats claimed, "while ISIS is nearing territorial defeat in Iraq and Syria, the group has returned to its guerilla warfare roots while continuing to plot attacks and direct its supporters worldwide."[69] Overseas terrorism remains a threat to the United States, but may not be as imminent a threat.

In his Naval Postgraduate School thesis, Matthew Jackson contended, "even though almost all of their [ISIS] territory has been lost, ISIS still poses a grave threat to the American homeland."[70] Mr. Jackson was further concerned about the "100,000 former ISIS fighters" who might be released from detention and "could recapture old territory and launch more attacks around the world."[71] The concern about current ISIS capabilities is not lost on the U.S. government. According to the *2021 IC Annual Threat Assessment*, America still faces threats from overseas terrorist groups, such as ISIS.[72] However, the assessment contends that "sustained U.S. and allied CT pressure has broadly degraded their

---

66 Trump, *National Strategy for Counterterrorism of the United States of America*, 7.

67 Mark Landler and Eric Schmitt, "Terrorist Threat 'More Fluid and Complex than Ever,' White House Says," *New York Times*, sec. United States, para. 2, October 4, 2018, https://www.nytimes.com/2018/10/04/us/politics/trump-counterterrorism-strategy.html. Webpage quote found in 2nd paragraph.

68 Daniel R. Coats, *DNI Coats Opening Statement on the 2019 Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2019), 19, https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1949-dni-coats-opening-statement-on-the-2019-worldwide-threat-assessment-of-the-us-intelligence-community.

69 Coats, 19.

70 Matthew L. Jackson, "America's Three Domestic Threats and the Need for a Reform of Domestic Intelligence" (master's thesis, Naval Postgraduate School, 2020), 12, https://calhoun.nps.edu/bitstream/handle/10945/66087/20Sep_Jackson_Matthew.pdf?sequence=1&isAllowed=y.

71 Jackson, 12.

72 Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2021), https://www.hsdl.org/?abstract&did=852427.

[ISIS] capability," and that "U.S.-based lone actors and small cells with a broad range of ideological motivations pose a greater immediate domestic threat."[73]

The United States is no longer concerned with solely countering threats from overseas terrorist organizations akin to al-Qaeda and ISIS. In 2014, Mike German, a Fellow at the Brennan Center for Justice, interviewed author and professor Dr. Erik Dahl who stated, "the nature of the domestic terrorism threat in the United States today is actually more serious, more severe than many believe it is—especially when you consider that there are a number of plots that have been thwarted since 9/11 from domestic right-wing or other sorts of organizations."[74] Dr. Dahl is not alone in this belief. Indeed, right-wing groups in America associate with "violence at all levels and seem to view violence as axiomatic in the movement," according to Christopher Adamczyk in his master's thesis.[75] Further, Mr. Adamczyk stated, "groups like RTT [Revolt through Tradition], the AWD [Atomwaffen Division], even Patriot Front revel in violence and…motivate adherents to commit violent acts."[76] According to a 2021 project by the think tank New America, since 2001, "far-right terrorism," which includes "anti-government, militia, white supremacist, and anti-abortion violence," has killed 114 people in the United States, compared to 107 people killed in the United States by jihadist militants during the same timeframe.[77] In line with the New America report, Michael C. McGarrity, former Assistant Director of the FBI's Counterterrorism Division (2018–2019), in May 2019 told the U.S. House Homeland Security Committee "domestic terrorists pose a present and persistent threat of violence and economic harm."[78] Mr. McGarrity indirectly confirmed the New America reporting in

---

[73] Office of the Director of National Intelligence, 23.

[74] Mike German, "Rethinking Intelligence: Interview with Erik Dahl," para. 20, Brennan Center for Justice, June 6, 2014, https://www.brennancenter.org/our-work/research-reports/rethinking-intelligence-interview-erik-dahl.

[75] Christopher J. Adamczyk, "Gods versus Titans: Ideological Indicators of Identitarian Violence" (master's thesis, Naval Postgraduate School, 2020), 54, https://www.hsdl.org/?abstract&did=847107.

[76] Adamczyk, 54.

[77] Peter Bergen et al., "Part IV. What Is the Threat to the United States Today?," New America, para. 3, 2021, http://newamerica.org/in-depth/terrorism-in-america/what-threat-united-states-today/.

[78] McGarrity, "Confronting the Rise of Domestic Terrorism in the Homeland," para. 4.

his statement to the committee that "there have been more arrests and deaths caused by domestic terrorists than international terrorists in recent years."[79]

In contrast, the American Civil Liberties Union (ACLU), while not discounting the domestic terrorism threats, has written that the definition of domestic terrorism is too liberal.[80] The ACLU states that Public Law 107-52 (USA PATRIOT ACT) allows for the prosecution of domestic terrorism when an individual's acts are "dangerous to human life" and should only be applied when acts "cause serious physical injury or death."[81] There appears to be grey area when considering which threats are more pervasive and of a higher priority.

To identify the U.S. threat priorities, the literature provides a definition of the National Intelligence Priorities Framework (NIPF). The *2018 National Counterintelligence and Security Center Strategic Plan* defines the NIPF as a mechanism that "reflects policymakers' priorities for national intelligence support and ensures that enduring and emerging intelligence issues are addressed."[82] Further, former Director of Central Intelligence (DCI), George Tenet (1997–2004) described the NIPF "as being more flexible and more precise than any previous intelligence priority system."[83] The details of the NIPF are classified and therefore this thesis is unable to list the actual intelligence priorities. However, the absence of classified details does not detract from the thesis' analysis.

---

[79] McGarrity, para. 4.

[80] The ACLU believes that the Section 802 of the USA PATRIOT Act (Public Law 107-52) definition of domestic terrorism is written "broad enough to encompass the activities of several prominent activist campaigns and organizations. Greenpeace, Operation Rescue, Vieques Island, and WTO protesters and the Environmental Liberation Front have all recently engaged in activities that could subject them to being investigated as engaging in domestic terrorism." "How the USA PATRIOT Act Redefines 'Domestic Terrorism,'" American Civil Liberties Union, accessed June 14, 2021, https://www.aclu.org/other/how-usa-patriot-act-redefines-domestic-terrorism.

[81] American Civil Liberties Union, para. 1.

[82] William R. Evanina, *National Counterintelligence and Security Center Strategic Plan, 2018–2022* (Washington, DC: National Counterintelligence and Security Center, 2018), 12, https://www.odni.gov/files/NCSC/documents/Regulations/2018-2022-NCSC-Strategic-Plan.pdf.

[83] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 7th ed. (Los Angeles: QC Press, 2017). The NIPF "allowed policy makers and intelligence officers to identify the countries or non-state actors of interest and their activities that are of interest and then to give them relative levels of importance as intelligence priorities." Lowenthal, XX.

However, the *2019 United States National Intelligence Strategy*, which supports national security priorities, addresses the "threats [which] are becoming ever more diverse and interconnected," to include traditional adversaries like Russia, China, Iran, and North Korea, as well as cyber threats, emerging technologies, violent extremist groups, and the increase in migration and urbanization populations.[84] Looking further, the IC's *2019 World Threat Assessment* (WTA), puts a significant precedence on traditional state actors. The WTA, like the NIS, sees Russia, China, Iran, and North Korea as imminent and long-term adversaries using multiple threat scenarios against the United States.[85] The WTA does address overseas terrorist organizations, homegrown violent extremists (HVEs), counterintelligence, and emerging and disruptive technologies, but is focused on the actions from state-level actors.[86] The WTA does not advertise how the United States, specifically the IC, plans to respond to today's threats.

While overseas terrorism, domestic terrorism, and traditional threat actors are high priority targets for the U.S. government, the threat from TOCs pose just as much risk. The TSA is not immune from the threats presented by TOCs. According to the Global Initiative against Transnational Organized Crime, TOC actors' use of "air travel has been a key conduit of illicit goods, most of which goes undetected," and the majority of the movement of illicit goods "take place on commercial airlines."[87] A recent report by RAND presents the emergent threat of TOC actors as a "hybrid" that "combines aspects of criminal organizations, terrorist groups, and insurgencies," and believes TOCs "pose crosscutting threats to U.S. security interest."[88]

---

84 Coats, *National Intelligence Strategy of the United States of America*, 4.

85 Daniel R. Coats, *Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, DC: Office of the Director of National Intelligence, 2019), 5–11, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

86 Coats, 12–13.

87 Summer Walker et al., *The Global Illicit Economy: Trajectories of Transnational Organized Crime* (Geneva, Switzerland: Global Initiative against Transnational Organized Crime, 2021), 26, https://globalinitiative.net/wp-content/uploads/2021/03/The-Global-Illicit-Economy-GITOC-Low.pdf.

88 Rabasa et al., *Counternetwork*, XVI.

Viewing TOCs as a hybrid has not gone unnoticed at the TSA. Over the last seven years, according to the TSA's *Insider Threat Roadmap*, the TSA has encountered several incidents involving TOC actors. One example, as mentioned in Chapter I was a 2018 event that busted several airline workers for smuggling illegal drugs, for a TOC group, onto departing aircraft.[89] This illegal activity not only involved TOC actors, but the recruitment of insiders who exploited their access to secure areas within an airport for illegal activity. In some cases, the insiders transported, carried, or passed along prohibited or dangerous items.[90] Along with the TOC and insider threat, the TSA is concerned that a "terrorist could exploit the tactics, techniques, and procedures used by the transnational criminal organizations" in an effort to recruit credentialed TSA insiders.[91]

B. INTELLIGENCE COMMUNITY TODAY

This thesis proposes that the TSA is not only an airport security administration, but it can also contribute more to U.S. national security. The TSA was formed because of the attacks in 2001. Its mission is heavily focused on airport security. However, Chapter I provided examples of the threats facing the TSA today, from overseas terrorist organizations, domestic terrorists with a spectrum of ideological beliefs, to TOC actors and the insider threat actors willing to take advantage of their privileged access. The examples in Chapter I show how the TSA is responding to a wide range of complex threats, both domestically and overseas, and how the TSA's mandate from 20 years ago has shifted. Just as the IC and the members within the IC have transformed over the last two decades, the TSA in 2021, needs to make organizational changes to support the IC better.

Today's IC looks different than it did 20 years ago. The IC is now led by the DNI, as opposed to the DCI. The IC has more statutory members, such as the Space Force. The 2021 intelligence budget was just under 86 billion dollars, which continually increased over the 20 years, and might be necessary to confront all the existing threats to the United

89 Pekoske, *Insider Threat Roadmap 2020*, 6.

90 Pekoske, 6.

91 Pekoske, Executive Summary, 3.

States.[92] According to the *Homeland Security Affairs* journal, most of the changes in the IC occurred due to a strategic event, such as the 1941 Pearl Harbor attack, or the al-Qaeda attack in 2001. Both of these events shook America, and "serve [d] as the impetus to reevaluate national policies," and "alter strategic policy in a fundamental ways."[93] The TSA was created due to such a devastating attack on America. A new attack however should not have to occur for the TSA to transform its capabilities.

In her speech to the Senate Committee on Commerce, Science, and Transportation, TSA former Acting Deputy Administrator Patricia F. S. Cogswell stated, "TSA's continued success is contingent upon our ability to rise to the challenge of outmatching a dynamic threat to our aviation and surface transportation systems."[94] Going further, TSA Administrator David Pekoske told the U.S. Senate, "to be effective and efficient in a changing environment, TSA must continuously re-evaluate how it [TSA] uses its resources and performs its mission."[95] For the TSA to support the IC efforts, by enhancing the TSA's intelligence functions, fundamental changes need to be made within the organization. Based on the previous comments, the TSA is aware change should occur. Over the years, the IC has transformed either by a tragic event, or by choice.

While not on the same scale, the TSA can follow the lead of the CIA by choosing to modify its organization to meet the challenges of tomorrow. Citing the need to adapt to surging threats, Greg Miller of the *Washington Post* reported, "the CIA unveiled a radically altered org chart," which came complete with "the most ambitious addition…the

---

92 "IC Budget, What We Do," Director of National Intelligence, 2021, https://www.dni.gov/index.php/what-we-do/ic-budget.

93 James Burch, "The Domestic Intelligence Gap: Progress since 9/11?," *Homeland Security Affairs* XVII (April 1, 2008): 1, https://www.hsaj.org/articles/129.

94 Patricia F. S. Cogswell, "Protecting the Nation's Transportation Systems: Oversight of the Transportation Security Administration," para. 11, Transportation Security Administration, September 11, 2019, https://www.tsa.gov/news/press/testimony/2019/09/11/protecting-nations-transportation-systems-oversight-transportation.

95 David Pekoske, "Keeping Our Skies Secure: Oversight of the TSA," para. 8, Transportation Security Administration, September 5, 2018, https://www.tsa.gov/news/press/testimony/2018/09/05/keeping-our-skies-secure-oversight-tsa.

Directorate of Digital Innovation [DDI]."[96] The DDI is an answer to the fact that "the CIA's mission is under digital assault."[97] The DDI architect, former CIA Director John Brennan (2013–2017), advocated for breaking down "the silos and cultural blockades" that impeded the agency's abilities.[98] Through such transformation, Mr. Brennan believes "agencies are better able to connect data points," and "if the same data points that were available prior to 9/11 were available today, there never would have been a 9/11."[99] Truly a bold comment.

Respected author Amy Zegart and former Deputy Director and Acting Director of the CIA Michael Morell (2012–2013) recognize the shifting threat landscape and agree that the IC needs to transform to meet the challenge. However, Zegart and Morell believe the intelligence agencies have not progressed quickly enough.[100] They point to the Russian interference in the 2016 U.S. presidential election and see that interference as a current intelligence failure.[101] These types of gaps need to be filled.

Identifying an opportunity to enhance agencies' capabilities to defend the homeland is imperative for the TSA to defeat the threats identified in Chapter I. The TSA, while nascent in intelligence experience, is a readily available U.S. government asset that can extend its current mission in support of the IC.

C. TSA'S CURRENT ROLE IN INTELLIGENCE

The literature on the TSA's intelligence role is limited in the public forum because the TSA's intelligence work is classified. However, the DHS Office of Inspector General

---

96 Greg Miller, "The CIA Unveils a Radically New Org Chart," *Washington Post*, sec. Military, para. 1, 4, October 1, 2015, https://www.washingtonpost.com/news/checkpoint/wp/2015/10/01/the-cia-unveils-a-radically-new-org-chart/.

97 Miller, para 5.

98 Bradley Barth and Teri Robinson, "Former CIA Director Brennan Recounts His Transformation into a Full-Fledged Cyber Strategist," para. 1, SC Media, October 10, 2018, https://www.scmagazine.com/news/-/former-cia-director-brennan-recounts-his-transformation-into-a-full-fledged-cyber-strategist.

99 Barth and Robinson, para 2.

100 Amy Zegart and Michael Morell, "Spies, Lies, and Algorithms," 1, *Foreign Affairs*, May 28, 2019, https://www.foreignaffairs.com/articles/2019-04-16/spies-lies-and-algorithms.

101 Zegart and Morell, 1.

(DHS OIG) states the TSA's Office of Intelligence and Analysis (TSA I&A) mission "is to identify security risks to prevent attacks against the United States transportation system."[102] The Heritage Foundation's, David Inserra, a former policy analyst for homeland security and cyber policy, believes the TSA is strictly a security agency focused on aviation, and therefore, "privatizing the TSA would result in savings that could be reinvested in more effective homeland security programs that need the additional funding and could also improve security across the U.S."[103] However, the literature shows the TSA plays a part in multiple transportation vectors. The Office of the Federal Register indicates that the "TSA employs a risk-based strategy…working closely with stakeholders in aviation, rail, transit, highway, and pipeline sectors, as well as the partners in the law enforcement and intelligence community."[104] Going further, the Register notes that the TSA "will continuously set the standard for excellence" with its "use of intelligence to drive operations."[105]

Senior government officials debate the TSA's expanded role in intelligence. For example, a December 2018 Government Accountability Office (GAO) report reviewed the TSA's intelligence cooperation with the U.S. interstate pipeline system. The report found TSA I&A "provide [s] pipeline industry security professionals with timely and actionable information on terrorist threats," and "provides quarterly intelligence briefings," regarding "threat actors, credible terrorist plots, and successful attacks."[106] While the report believes the TSA can be more engaged with the pipeline sector, the report notes that pipeline officials are less concerned with receiving additional TSA I&A intelligence guidance, as

---

[102] Office of the Inspector General, *TSA's Office of Intelligence and Analysis Has Improved Its Field Operations*, Report No. OIG-17-107 (Washington, DC: Department of Homeland Security, 2017), 2, https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-107-Sep17.pdf.

[103] David Inserra, "Time to Privatize the TSA," summary, The Heritage Foundation, July 19, 2017, https://www.heritage.org/homeland-security/report/time-privatize-the-tsa.

[104] National Archives and Records Administration, "Transportation Security Administration," para. 3, Federal Register, accessed December 3, 2020, https://www.federalregister.gov/agencies/transportation-security-administration.

[105] National Archives and Records Administration, para. 3.

[106] Government Accountability Office, *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, GAO-19-48 (Washington, DC: Government Accountability Office, 2018), 24, https://www.gao.gov/assets/700/696123.pdf.

"the threats to the oil and natural gas sector have been historically low."[107] However, in May 2021, the Colonial Pipeline Company had to cease its pipeline operations due to a ransomware attack, which caused delays in production and shipment of necessary oil along the U.S. Eastern Shore. A May 2021 report by the CRS concurs that all regulation between private stakeholders, such as the Colonial Pipeline Company and the U.S. federal government, have been on a voluntary basis for both physical security and cybersecurity.[108] Such an impactful incident should draw interest from both the private and public sectors to collect and share valuable intelligence.

In the same vein, Jesse Cohen points out that the TSA is "responsible for setting and managing the security programs" of not just passengers but also the screening of cargo shipments.[109] Cohen does not indicate whether cargo screening falls within the TSA's intelligence section. Recognizing however that the mission is "to detect and prevent explosives in a cargo shipment from boarding an aircraft, and to ensure the security of the crew," it is directly related to countering terrorism and the continued threat to the United States.[110]

In response to a House oversight committee hearing, former U.S. Representative John Mica (R-Fla) (1993–2017), stated that he would like to see the TSA hand over the screening business to private security companies and focus "on intelligence to identify and address threats."[111] Rep. Mica believes connecting the dots, through "handling classified information, information on terrorists, the ability to track people, to make sure the

---

[107] Government Accountability Office, 72.

[108] Paul W. Parfomak and Chris Jaikaran, *Colonial Pipeline: The DarkSide Strikes*, CRS Report No. IN11667 (Washington, DC: Congressional Research Service, 2021), 2, https://crsreports.congress.gov/product/pdf/IN/IN11667.

[109] Jesse Cohen, "Securing the Air Cargo Supply Chain," para. 1, Freight Waves, April 17, 2019, https://www.freightwaves.com/news/airfreight/securing-the-air-cargo-supply-chain.

[110] Cohen, para 5.

[111] Andrew Becker, "Lawmaker Says TSA Should Focus on Intelligence, Get out of Screening," para. 1, Reveal from the Center for Investigative Reporting, April 28, 2016, https://www.revealnews.org/blog/lawmaker-says-tsa-should-focus-on-intelligence-get-out-of-screening/.

(terrorist) watchlist is up to date, so people are identified even before they get to the airport," is of most value.[112]

To the public, the TSA appears to be a security organization constrained to U.S. airports whose expanded mission is limited. Taking into consideration the need to maintain privacy and limit the collection of information on U.S. citizens, who do not have a nexus to terrorism or are a national security threat, many Americans can be presumed hesitant if the TSA expands its intelligence responsibilities. The public's response to the TSA's Quiet Skies (QS) program is an indication.

Most of the authors who have written about the TSA have not covered the TSA's intelligence activities. However, after a 2018 open-source report detailed that the TSA Federal Air Marshal Service (FAMS) was conducting surveillance and documenting pattern-of-life and atmospheric data on non-watchlisted individuals, the DHS OIG opened an investigation.[113] The DHS OIG report found that the "TSA did not properly plan, implement, and manage the Quiet Skies program to meet the program's mission of mitigating the threat to commercial aviation posed by higher risk passengers."[114] Regardless of the DHS OIG report, many authors covering this story simply summarized the program as domestic surveillance. As of December 2018, the TSA has said it "curtailed its controversial 'Quiet Skies' domestic surveillance program."[115]

---

[112] Becker, para. 3.

[113] Office of the Inspector General, *TSA Needs to Improve Management of the Quiet Skies Program (Redacted)*, OIG-21-11 (Washington, DC: Department of Homeland Security 2020), 2–7, https://www.oig.dhs.gov/sites/default/files/assets/2020-11/OIG-21-11-Nov20-Redacted.pdf.

[114] Office of the Inspector General, 3.

[115] Jana Winter and Jenn Abelson, "TSA Says It No Longer Tracks Regular Travelers like Terrorists," para. 1, *The Boston Globe*, December 15, 2018, https://www.bostonglobe.com/news/nation/2018/12/15/curtails-quiet-skies-passenger-surveillance/2lRAv2AwjGpUcgq08mHaPM/story.html. "The Transportation Security Administration (TSA) leverages its access to the U.S. Customs and Border Protection (CBP) Automated Targeting System to identify individuals for enhanced screening during air travel through the use of rules based on current intelligence as part of its Secure Flight vetting process;" "Under TSA's Quiet Skies program, TSA uses a subset of Silent Partner rules to identify passengers for enhanced screening on some subsequent domestic and outbound international flights." Thomas Bush, *Privacy Impact Assessment Update for Secure Flight Silent Partner and Quiet Skies* (Washington, DC: Department of Homeland Security, 2019), 2, https://www.dhs.gov/sites/default/files/publications/pia-tsa-spqs018i-april2019_1.pdf.

Such activity caused concern with the public, and just adds to the suspicion people already maintain toward the TSA.[116] According to a 2019 ProPublica article, the TSA full-body scanners may have discriminated against African American women, due to certain types of headwear.[117] According to the Electronic Frontier Foundation, this type of reporting, expectedly, creates a backlash toward the TSA and allowed critics to surmise the TSA is already collecting too much invasive information.[118]

Upon moving further away from 9/11, many authors agree that the threats the United States faces are more diverse than just overseas terrorist organizations. Today's higher priority threats, such a domestic terrorism and transnational organized crime, have an impact on the TSA. Defeating the threats from overseas terrorist organizations will always be a priority for the TSA. The TSA can transform itself, as some members of the IC have done, so that the TSA can better position itself for the future.

D. CHAPTER SUMMARY

This chapter provided scholarly works that discussed the threats facing America. This chapter also discussed different authors and scholars' opinions on the IC's changes since 9/11. Finally, this chapter provided a review of the literature that discussed the TSA's current support to intelligence.

The next chapter presents the authorities that guide the TSA's operational activities, and the TSA's current role supporting the U.S. IC. Chapter III then provides an overview of the DHS Intelligence Enterprise (DHS IE), as well as the TSA's place within the DHS IE. Finally, Chapter III details the rules and regulation the TSA operates under and ends with a breakdown of the TSA's support to U.S. intelligence.

---

116 Office of the Inspector General, *Quiet Skies Program (Redacted)*, 2, 6–7, 9, 14.

117 Brenda Medina and Thomas Frank, "TSA Agents Say They're Not Discriminating against Black Women, but Their Body Scanners Might Be," ProPublica, April 17, 2019, https://www.propublica.org/article/tsa-not-discriminating-against-black-women-but-their-body-scanners-might-be.

118 India McKinney, "TSA's Roadmap for Airport Surveillance Moves in a Dangerous Direction," Electronic Frontier Foundation, December 7, 2018, https://www.eff.org/deeplinks/2018/12/tsas-roadmap-airport-surveillance-moves-dangerous-direction.

III. TSA TODAY: CURRENT OPERATIONS AND AUTHORITIES

This chapter discusses the authorities that guide the TSA's operational activities, and its current role supporting the U.S. national intelligence. It starts with an overview of the DHS IE, and a discussion of the TSA's place within the DHS IE. This chapter then details the rules and regulation the TSA operates under and ends with a breakdown of the TSA's support to U.S. intelligence.

To most people, the TSA is viewed strictly as a security agency that functions primarily within the U.S. airports. The public believes the TSA is only responsible for the screening of passengers and luggage. Since 9/11, the public and media discussions surrounding the TSA's creation have identified the entirety of the TSA in this manner. Some analysis reporting states that the TSA's existence is not justified, the TSA should be privatized, and the TSA's funding should be given to other DHS programs.[119] These issues were highlighted in Chapter II. However, the research for this thesis indicates the TSA is required by law to function beyond airport security to protect against threats to the American public and the U.S. transportation infrastructure.[120]

The majority of the TSA's workforce, approximately 50,000 employees, is composed of the visible Transportation Security Officers, who are focused on securing the sterile areas within U.S. airports.[121] An also unseen cadre of TSA employees is working to defeat threats before they reach the airports or the U.S. border. These officers have a mandate that extends beyond the transportation security realm, to include counterterrorism and counterintelligence operations, and their contributions support the U.S. government's work to defeat multiple threats through the collection, analysis, and dissemination of relevant intelligence.[122]

---

[119] Bruce Schneier, "Why Are We Spending $7 Billion on TSA?," CNN, June 5, 2015, https://www.cnn.com/2015/06/05/opinions/schneier-tsa-security/index.html.

[120] Aviation and Transportation Security Act of 2001, 2.

[121] "TSA by the Numbers," Transportation Security Administration, last updated May 19, 2021, https://www.tsa.gov/news/press/factsheets/tsa-numbers.

[122] Brian Bean, "Mitigating Insider Threats in the Domestic Aviation System: Policy Options for TSA," *Homeland Security Affairs* (blog), December 1, 2017, https://www.hsaj.org/articles/14380.

In the TSA's support to U.S. national security, the TSA's greatest attention is on defeating threats to the aviation ecosystem.[123] Most of the formidable threats are countered through the vetting of airline passengers, the forward and recurrent vetting of the credentialed transportation workforce, and the watchlisting of KSTs.[124]

The following section illustrates the DHS's place within the IC through the DHS I&A, the DHS I&A authorities within the IC, and the DHS I&A's and DHS IE's interactions with U.S. intelligence. This section then provides the TSA's related legislation to engage in intelligence activities, and the intelligence functions the TSA can and cannot perform.

A. TSA'S POSITION AND AUTHORITIES

The TSA, one component of the DHS, is a member of the DHS IE, yet not a statutory member of the IC. The DHS IE is comprised of the DHS components that support U.S. intelligence activities, including, for example, United States Citizenship and Immigration Services, United States Customs and Border Protection (CBP), Cybersecurity and Infrastructure Security Agency, Federal Emergency Management Agency, United States Immigration and Customs Enforcement, and the United States Secret Service.[125] Each of these components maintains at least one intelligence function, which is termed the Component Intelligence Program (CIP).[126] Each CIP provides the DHS with analysis and threat warnings on homeland security priorities relevant to each component's mission, and propagates the sharing of information with multiple government partners.[127] The DHS IE

123 Trump, *National Strategy for Aviation Security of the United States of America*, 1.

124 Transportation Security Administration, *Budget Overview: Fiscal Year 2020 Congressional Justification* (Washington, DC: Department of Homeland Security, 2020), 5, https://www.dhs.gov/sites/default/files/publications/19_0318_MGMT_CBJ-Transportation-Security-Administration_0.pdf.

125 "The Intelligence Enterprise," Department of Homeland Security, August 8, 2019, https://www.dhs.gov/intelligence-enterprise. The United States Coast Guard (USCG) is not only a component of the DHS, making its intelligence unit a member of the IE, but the USCG is one of the 17 statutory IC members.

126 Majority Staff of the House Homeland Security Committee, *Reviewing the Department of Homeland Security's Intelligence Enterprise* (Washington, DC: Homeland Security Committee, 2016), 11, 14–16, https://www.hsdl.org/?view&did=797351.

127 Randol, *The Department of Homeland Security Intelligence Enterprise*, 19.

falls under the umbrella of the DHS I&A, which is a statutory member of the IC.[128] The DHS I&A's statutory IC membership provides a pathway for each CIP member to provide intelligence collection to contribute to improved IC analysis of potential threats to the United States' national security. This thesis argues that the pathway to the IC is an opportunity for the TSA to expand its intelligence capabilities with existing legal authorities and policies.

Currently, 18 agencies make up the U.S. IC, which include two independent agencies, the ODNI and the CIA.[129] Additionally, the Department of Defense (DOD) has nine IC organizations: the Defense Intelligence Agency, the National Security Agency, the National Geospatial-Intelligence Agency, the National Reconnaissance Office, and five intelligence elements within each of the military services, which includes the newest IC member, the Space Force.[130] Additionally, seven IC members fall within larger organizations that maintain functions outside of intelligence, which include the Department of Energy's Office of Intelligence and Counterintelligence, USCG Intelligence, Department of Justice's FBI National Security Branch, the Drug Enforcement Administration's (DEA's) Office of National Security Intelligence, Department of State's Bureau of Intelligence and Research, Department of the Treasury's Office of Intelligence and Analysis, and the DHS I&A.[131]

When the DHS was established, it was designed to be "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[132] While considered a colossal task, the DHS was created as a headquarters element responsible for multiple incoming components, even subsuming the newly created TSA from the

---

128 Randol, 17.

129 "Members of the IC," Office of the Director of National Intelligence, March 28, 2019, https://www.dni.gov/index.php/what-we-do/members-of-the-ic.

130 Office of the Director of National Intelligence.

131 Office of the Director of National Intelligence.

132 George W. Bush, *National Strategy for Homeland Security* (Washington, DC: White House, 2002), 2, https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf.

Department of Transportation.[133] Each of these components, sans the TSA, joined the ranks of the DHS having held long established processes and independent organizational identities, with some already having established intelligence functions. The blending of the DHS CIPs with the DHS I&A has been an ongoing process. No formal legislation has been established to standardize the national intelligence cycle at the department level to which the DHS IE can adhere. The following section discusses the DHS I&A charter and how it engages with the DHS IE.

1. DHS I&A and the Intelligence Enterprise

The DHS I&A represents the entire DHS for the IC, and is tasked with collecting, analyzing, and disseminating intelligence for the DHS to the IC.[134] Multiple laws and regulations, including the Homeland Security Act of 2002, give the DHS I&A its charter to identify and deter threats that come from within the borders of the United States. Together, these laws, such as Executive Order (EO) 12333, as well as the NSA 47, provide the direction and oversight instructions that guide the DHS I&A to fulfill its national security requirements.[135] The DHS I&A is required to support national security through the collection and analysis of information gathered at the department and field levels.

For the last 19 years, the DHS I&A has taken on multiple roles within the DHS. At times, the DHS I&A functions as a headquarters element that maintains a strategic posture,

---

133 Marisa Mullen, "Transportation Security Administration Transition to Department of Homeland Security; Technical Amendments Reflecting Organizational Changes," National Archives, Federal Register, August 19, 2003, https://www.federalregister.gov/documents/2003/08/19/03-20927/transportation-security-administration-transition-to-department-of-homeland-security-technical.

134 "Office of Intelligence and Analysis," Department of Homeland Security, June 18, 2015, https://www.dhs.gov/office-intelligence-and-analysis.

135 "The National Security Act of 1947 mandated major reorganization of the foreign policy and military establishments of the U.S. government. The act created many of the institutions that Presidents found useful when formulating and implementing foreign policy, including the National Security Council (NSC)…The act also established the Central Intelligence Agency (CIA), which grew out of World War II era Office of Strategic Services and small post-war intelligence organizations." "Milestones: 1945–1952 National Security Act of 1947," 1, Office of the Historian, accessed December 12, 2020, https://history.state.gov/milestones/1945-1952/national-security-act. EO 12333 is a foundational presidential order that defines the "goals, directions, duties, and responsibilities with respect to United States intelligence efforts." Ronald Reagan, Executive Order 12333, "United States Intelligence Activities," National Archives, December 4, 1981, https://www.archives.gov/federal-register/codification/executive-order/12333.html.

guides the DHS components with ad-hoc requirements, and extends its analysis and capabilities to the CIP. This structure is similar to that of the DOD. The Department of the Army, Department of the Navy, and Department of the Air Force all report to the DOD. Other times, the DHS I&A positions itself in a support role to the DHS components, as well as provides non-strategic intelligence to state, local, and tribal affiliates. As such, the DHS I&A is unique among the other IC members. For example, the DHS I&A was integral in the creation of the national fusion centers and the communication network to pass along sensitive but unclassified information to mission partners.[136] The DHS I&A has not been able to stick with one role because no legislation requires the DHS to unify the DHS IE regarding engagement with the DHS IE components.

However, in 2020, the U.S. Senate passed the Unifying DHS Intelligence Components Act (UDHSIC) to govern and provide direction throughout the department's intelligence activities, as it pertains to standardizing intelligence collection and analysis training.[137] However, this act limits the possibility to unite the DHS IE. Intelligence priorities and requirements fundamental in directing an intelligence organization in its collection efforts are not addressed.

Setting strategic priorities for an intelligence organization is necessary for the organization to understand the direction it is going. The DHS I&A Strategic Plan for Fiscal Year 2011–2018 noted the DHS created a Homeland Security Intelligence Priority Framework (HSIPF). The research however does not show that the framework has been

136 Todd Rosenblum, "Inside DHS' Intelligence Mission," The Cipher Brief, August 29, 2018, https://www.thecipherbrief.com/column_article/inside-dhs-intelligence-mission. "Fusion Centers are state-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between state, local, tribal and territorial (SLTT), federal and private sector partners." "Fusion Centers," Department of Homeland Security, July 6, 2009, https://www.dhs.gov/fusion-centers. The "communication network" refers to the DHS's Homeland Security Information Network (HSIN), used to share information between the DHS and state, local, territorial, tribal, international, and private sector partners. "Homeland Security Information Network (HSIN)," Department of Homeland Security, November 19, 2014, https://www.dhs.gov/homeland-security-information-network-hsin.

137 United States Senate, *Unifying DHS Intelligence Components Act* (Washington, DC: United States Government Publishing Office, 2020), 1, https://www.hsdl.org/?abstract&did=853607.

incorporated throughout the DHS IE.[138] In this plan, the HSIPF was defined as a "unified set of homeland security information priorities" within the IC. The HSIPF is not dependent on, but linked to, the NIPF.[139] However, this plan did not explain how the HSIPF was used and if it was used by the DHS CIP units within DHS I&A.[140] Additionally, and like the UDHSIC Act, this plan made no mention of transportation intelligence requirements that the TSA could use to guide its intelligence collection. This type of structure and operating procedure has created gaps in intelligence collection and has led to criticism of the overall intelligence products the DHS I&A has produced.[141]

Indeed, in a 2011 review of the DHS I&A's work, the Center for Investigative Reporting determined that the DHS I&A's intelligence products were not on par with the IC and did not provide much value to America's overall intelligence mission.[142] In this connection, Becker and Schultz note that the DHS I&A's intelligence "reports [to the IC] have been outdated, irrelevant or vague, or have regurgitated stories that appeared in the media," and thus equate I&A's work to "intelligence spam."[143] A more recent (2016) review by the House Homeland Security Committee determined that even though the DHS I&A improved the flow of intelligence, the DHS did not lead its IE appropriately. The DHS IE lacks direction in its missions, has not been provided a concrete intelligence policy, and the "unique contributions the [component intelligence units] can make to our nation's security…are not easily accessible."[144] While the DHS I&A has the charter to synthesize,

---

138 Caryn A. Wagner, *Office of Intelligence and Analysis Strategic Plan—Fiscal Year 2011–Fiscal Year 2018* (Washington, DC: Office of Intelligence and Analysis, Department of Homeland Security, 2011), 12, https://www.dhs.gov/xlibrary/assets/ia-fy2011-fy2018-strategic-plan.pdf.

139 Wagner, 12.

140 Wagner.

141 Government Accountability Office, *DHS Intelligence Analysis: Additional Actions Needed to Address Analytic Priorities and Workforce Challenges*, GAO-14-397 (Washington, DC: Government Accountability Office, 2014), 12, 14, https://www.gao.gov/assets/670/663794.pdf.

142 Andrew Becker and G. W. Schulz, "Homeland Security Office Creates 'Intelligence Spam,' Insiders Claim," Reveal from The Center for Investigative Reporting, November 30, 2011, https://www.revealnews.org/article/homeland-security-office-creates-intelligence-spam-insiders-claim/.

143 Becker and Schulz, para. 6.

144 Majority Staff of the House Homeland Security Committee, *Reviewing the Department of Homeland Security's Intelligence Enterprise*, 3.

evaluate, and disseminate intelligence that it garners from the DHS IE components, it has so far failed to coalesce all the components intelligence units into one functioning intelligence provider. In sum, a more refined structure of the DHS I&A and the components of the DHS IE, through legal or formal policy, could produce more thorough intelligence products to pave the way to ensure all avenues of intelligence collection and dissemination occur.

2. TSA and its Operating Authorities

As is commonly known, the TSA was established after the terrorist attacks in 2001. The TSA acts as a deterrent to any future attacks on the U.S. transportation system through its operational and analytic activities. Several rules and regulations, including the Aviation and Transportation Security Act of 2001 (ATSA), give the TSA its ability to protect against the threats to America's public transportation sector. These authorities work in conjunction with one another. For example, some pieces of legislation, like EO 12333 and the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), were enacted to regulate or guide intelligence activities, while the others were created specifically to address the DHS and the TSA. The Homeland Security Presidential Directive 6 (HSPD-6) and the Memorandum of Understanding (MOU) on the Integration and Use of Screening Information to Protect against Terrorism were written to mandate the TSA to share terrorism information with the national security community. Finally, the Federal Aviation Administration Extension, Safety, and Security Act (FAA ESSA) of 2016 guides the TSA on the vetting operation for individuals seeking or currently working in the credentialed transportation workforce.

In line with ATSA, the TSA fulfils the following tasks that include providing security for the U.S. public transportation sector, screening operations for all passenger and intrastate air transportation, and controlling access to secure areas in an airport.[145] Most people are familiar with these actions and exposed to them daily within the airports.

[145] Aviation and Transportation Security Act of 2001, 10.

However, in 2004, the U.S. Congress released the IRTPA legislation to reform the IC.[146] The IRTPA provided instruction and guidelines to the TSA on aviation security, air cargo security, and maritime security to enhance security measures to the transportation sector.[147]

Through the IRTPA legislation, the TSA was directed to establish a pre-flight passenger prescreening program that compared both domestic and international traveler information to the No-Fly and Selectee sections of the Terrorist Screening Center's (TSC) consolidated watchlist (TSDB).[148] The pre-flight passenger prescreening program is known as Secure Flight.[149] Further, IRTPA allows the TSA to maintain sub-programs within Secure Flight to pre-screen individuals "against the full TSDB or other records," when necessitated by security considerations.[150] These sub-programs of Secure Flight are known as Silent Partner (SP) and QS.[151] As noted, the Secure Flight travel information is vetted against the TSC's watchlist, and when a match results, or possible match against the watchlist, the TSA sends the encounter notification to the TSC, and may be assumed to be disseminated within the IC, if required.[152] As a function of the Secure Flight program, the TSA reports that the FAMS submits after actions reports (AARs) on KST subjects that the FAMS has covered on a flight or in an airport.[153] Given a FAMS law enforcement

---

146 Intelligence Reform and Terrorism Prevention Act of 2004, *U.S. Code* 153 (2004), §§ 3001 50 https://legcounsel.house.gov/Comps/Intelligence%20Reform%20And%20Terrorism%20Prevention%20Act%20Of%202004.pdf.

147 Senate and House of Representatives of the United States of America in Congress.

148 Thomas Bush, *Privacy Impact Assessment Update for Secure Flight* (Washington, DC: Department of Homeland Security, 2017), 1–2, https://www.dhs.gov/sites/default/files/publications/pia_tsa_secureflight_18%28h%29_july2017.pdf. "The Terrorist Screening Center, a multi-agency center administered by the FBI, is the U.S. Government's consolidated counterterrorism watchlisting component and is responsible for the management and operation of the Terrorist Screening Database, commonly known as 'the watchlist'." "Terrorist Screening Center," Federal Bureau of Investigation, accessed July 5, 2021, https://www.fbi.gov/about/leadership-and-structure/national-security-branch/tsc.

149 Bush, *Privacy Impact Assessment Update for Secure Flight*, 1.

150 Bush, *Privacy Impact Assessment Update for Secure Flight Silent Partner and Quiet Skies*, 5.

151 Bush, 1.

152 Bush, 7. Secure Flight is built on privacy and the TSA only collects specific information for screening and vetting purposes, such as name, date of birth, gender, travel documentation, etc.

153 Bush, 4, 9, 11.

background, the AARs may contain additional information on the KST subject, such as atmospheric data (appearance, demeanor, etc.), as well as associations with other individuals of interest to the IC. If not already, the TSA's intelligence unit could serialize the AAR and use the information to write an Intelligence Information Report (IIR) and disseminate the raw intelligence to the IC.[154] Such intelligence could have value to the right government agency, which could lead to operational action against subjects of interest.

According to HSPD-6 and the MOU, once a passenger is confirmed as a KST identity, the TSA is required to relay collected terrorist information that meets the watchlisting guidance criteria. This information is submitted as a nomination to the National Counterterrorism Center's (NCTC) TIDE, which is an IC consolidated, classified terrorism identities database.[155] The NCTC then submits unclassified person identifiers to the TSC for inclusion in the TSDB, which is then exported to the unclassified screening and vetting systems. Nominations can include new person identities associated with terrorism, or enhancements to existing person terrorism records.[156]

This activity, known as watchlisting, is permitted by the TSA through EO 12333 since the TSA is a member of the DHS IE. Individuals identified by SP or QS rules program are not considered KSTs The information collected by Secure Flight is not sent to the NCTC. The information on SP and QS subjects does not contain adequate derogatory information that qualifies an individual to meet the reasonable suspicion standard outlined

---

154 "The Intelligence Information Report (IIR) is a raw intelligence report formatted as a teletype message that complies with specifications developed by the Defense Intelligence Agency (DIA) for the Intelligence Community (IC). The term 'raw intelligence' is defined as a colloquial term meaning unevaluated intelligence information, generally from a single source, that has not fully been evaluated, integrated with other information, or interpreted and analyzed." Department of Justice, *Request for Records Disposition Authority*, Standard Form 115 (REV 3 91) (College Park, MD: National Archives & Records Administration, 2010), 2, https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0065/n1-065-10-025_sf115.pdf.

155 George W. Bush, *Homeland Presidential Security Directive 6—Directive on Integration and Use of Screening Information to Protect against Terrorism* (Washington, DC: U.S. Government Publishing Office, 2003), https://www.govinfo.gov/content/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1174.pdf; National Counterterrorism Center, *Terrorist Identities Datamart Environment (TIDE)* (Washington, DC: Office of the Director of National Intelligence, 2017), 1–2, https://www.dni.gov/files/NCTC/documents/features_documents/TIDEfactsheet10FEB2017.pdf.

156 Bush, *Homeland Presidential Security Directive 6*, 1.

in the watchlisting guidance.[157] For example, travelers whose flights resemble a known flight pattern used by identified terrorist organizations may find themselves on either the SP or QS list. This information however alone does not qualify the individuals for watchlist nominations.[158] While a SP or QS person of interest does not meet the minimum watchlist nomination threshold, and is not nominated for inclusion in the TSDB, the information collected has potential value to the IC. The TSA should consider preparing an analytic report or IIR for IC dissemination. Additional analytical reporting opportunities are discussed in the next section.

Finally, the FAA ESSA mandates the TSA to vet individuals seeking or currently working in the credentialed transportation workforce. The FAA ESSA requires the TSA to complete a security threat assessment (STA) to ascertain the risk posed by an individual with access to the secure side of an airport. FAA ESSA also directs the TSA to compare current threat streams with the requirements needed to be eligible for an aviation worker credential, as well as creating or adopting industry standards for measuring access to the secure side of an airport and improving the review of the aviation workforce.[159] The TSA's vetting operations are continuously vetting credentialed employee records against the TSDB and the National Crime Information Center, for the period during which the STA is valid.[160] The TSA's vetting operations ensure that insider threats to aviation security are adequately addressed. Indeed, the TSA's vetting operations provide an excellent platform on which the TSA can expand its intelligence functions. The TSA is processing most of the vetting information on United States Persons (USPERs). USPER is a category of individuals on whom the IC can collect, but with greater restrictions than the TSA, per EO

---

157 Bush, *Privacy Impact Assessment Update for Secure Flight Silent Partner and Quiet Skies*. "Terrorist information" is defined as "information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism." Bush, *Homeland Presidential Security Directive 6*, 6.

158 Bush, *Privacy Impact Assessment Update for Secure Flight*, 2.

159 Serge Potapov, *Privacy Impact Assessment for the Insider Threat Unit Database* (Washington, DC: Department of Homeland Security, 2018), 2, https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa048-april2018.pdf.

160 "Recurrent Vetting," Transportation Security Administration, accessed July 5, 2021, https://www.tsa.gov/travel/frequently-asked-questions/recurrent-vetting.

12333. Such access to potential targets of interest with derogatory information, both domestically and overseas, presents opportunities to collect additional overt information that can add value to the IC. Serializing pertinent information from the TSA's vetting cycle can also add value to the IC. Additional vetting opportunities are discussed in the following section.

B. TSA'S SUPPORT TO INTELLIGENCE

The TSA plays an instrumental role in supporting the efforts of the nation's intelligence collection. Currently, all the intelligence functions inside the TSA reside with the TSA I&A. According to a recent review by the Homeland Security Committee, the TSA I&A has over 700 employees, with over 200 CIP personnel.[161] These members are spread out over multiple divisions and branches and include the Field Intelligence Integration Division (FIID), the Transportation Analysis Division (TAD), three around-the-clock watch floors, and the Vetting Analysis Division (VAD).[162] Each contributes unique transportation intelligence to the national intelligence and law enforcement communities. The following paragraphs provide the functions of the TSA's intelligence divisions and watch floors, as well as the extent of the TSA's input to the U.S. national intelligence.

The FIID works primarily through their Field Intelligence Officers (FIOs), with some headquarters personnel.[163] The FIOs work within the U.S. airport environments and ensure senior TSA leadership stays informed on all intelligence and threat matters, as well as provide local authorities with need-to-know updates that can affect a stakeholder's

---

[161] Majority Staff of the House Homeland Security Committee, *Reviewing the Department of Homeland Security's Intelligence Enterprise*, 11.

[162] Office of the Inspector General, *TSA's Office of Intelligence and Analysis Has Improved Its Field Operations*; Office of the Inspector General, *TSA Can Improve Aviation Worker Vetting (Redacted)*, OIG-15-98 (Washington, DC: Department of Homeland, 2015), 2, 9, https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-98_Jun15.pdf.

[163] According to the TSA's Fiscal Year 2020 Budget Overview, the TSA has requested to "eliminate its Field Intelligence Integration Division Headquarters positions in an effort to restructure delivery of support services within the field." Transportation Security Administration, *Budget Overview*, 36, 42, 50, 135, 169, 171.

interests.[164] According to a recent job posting, the FIO position is also required to liaise with the FBI's Joint Terrorism Task Force and the intelligence fusion centers.[165] The FIO's typical assignments include, "serving as a principal technical advisor on intelligence," and "developing high level briefs…[for] the identification, consideration, and resolution of real or potential security threats."[166] However, if not already doing so, the FIOs represent an excellent platform for the TSA to increase its intelligence collection to include strategic debriefing.[167] According to a 2017 DHS OIG report, the TSA only hires FIOs who have a deep understanding and experience in intelligence work. The FIOs must also demonstrate experience with supporting intelligence operations, preparing analytic briefs, assessing intelligence sources, as well as writing intelligence reports, such as the IIR.[168] Chapter V provides a recommendation for expanding the FIOs' intelligence roles within the TSA.

In addition to overseeing the FIO program, the FIID maintains a presence at the 24/7 Transportation Security Operations Center (TSOC).[169] The TSOC focuses on supporting security and intelligence operations in real-time, and in doing so, coordinates with multiple agencies on all aviation and transportation related events, operations, and emergency responses.[170] The TSOC remains operationally ready with up-to-date intelligence and

---

164 Office of the Inspector General, *TSA's Office of Intelligence and Analysis Has Improved Its Field Operations*, 2.

165 "Intelligence Operations Specialist—SV-0132-J—Career's, Women's Job List," Transportation Security Administration, April 8, 2015, https://www.womensjoblist.com/jobs/21478890/Intelligence-Operations-Specialist-SV-0132-J/.

166 Transportation Security Administration, heading Duties.

167 "Strategic debriefing is an interview activity conducted to collect information or to verify previously collected information in response to national or theater level collection priorities. This [strategic debriefing] avoids surprises of a strategic nature and is used to support long-range strategic planning. Strategic debriefing is conducted in peacetime as well as in wartime. It often fills gaps on extremely sensitive topics or areas…Debriefing operations often include the debriefing of personnel who may not usually be debriefed as part of their assigned duties." Department of the Army, *Human Intelligence Collector Operations*, vol. FM 34-35, Field Manual 2-22.3 (Washington, DC: Pentagon Library, 2006), 5–10, https://www.loc.gov/rr/frd/Military_Law/pdf/human-intell-collector-operations.pdf.

168 Office of the Inspector General, *TSA's Office of Intelligence and Analysis Has Improved Its Field Operations*, 3.

169 Office of the Inspector General, 2.

170 Transportation Security Administration, "TSA Transportation Security Operations Center: Still on Watch," *Transportation Security Administration* (blog), May 7, 2014, https://www.tsa.gov/blog/2014/05/07/tsa-transportation-security-operations-center-still-watch.

serves as the primary transportation security liaison for law enforcement and national intelligence. The TSA's TSOC maintains access to a web-based system (WebEOC) that receives information from multiple sources, to include authorities at the federal level through the tribal level, as well as from the private sector and international sources.[171] The TSA's Secure Flight provides the TSOC, through WebEOC, with the identities of travelers who match the TSDB (KSTs). The TSOC is then allowed to transmit this intelligence to the FIOs and FAMS so they remain knowledgeable and respond to incidents that may affect their areas of operation.[172]

Two more 24/7 watch floors are manned within the TSA. The Indications and Warning Watch (IWW), which is run by the TAD, provides the TSA leadership, and the National Transportation Vetting Center (NTVC), with high-level threat information on the transportation sector.[173] The IWW is vital to national intelligence. The IWWrelays actionable intelligence quickly to senior leaders in the TSA who are then able to coordinate with external agencies at a higher level. For example, the IWW, in coordination with the TSOC and NTVC, would have likely been involved in communicating up-to-the-minute intelligence to the TSA senior leadership during the 2021 Capitol Hill riots. Aside from running the IWW, the TAD maintains the SP and QS programs and is responsible for all strategic intelligence production coming from the TSA.[174] The intelligence production from TAD is provided to other TSA offices, the TSA workforce at the airports, and to appropriately cleared transportation stakeholders like passenger airlines, cargo airlines, rail

---

171 "Web-Based Emergency Operations Center (WebEOC) to store real-time information from federal, state, local, tribal, foreign, and international sources and private sector security officials to assist in performing transportation security functions. WebEOC stores information on individuals and witnesses involved in security incidents including: 1) individuals who violate or are suspected of violating transportation security laws, regulations, policies, or procedures; 2) individuals whose behavior or suspicious activity results in referrals to a Behavior Detection Officer or Law Enforcement Officer; and 3) individuals whose identity must be verified or checked against federal watch lists, including individuals who fail to show acceptable identification documents to compare to boarding documents and law enforcement officials who seek to fly armed." John Bogers, *Privacy Impact Assessment Update for the TSA Operations Center Incident Management System* (Washington, DC: Department of Homeland Security, 2015), 1, https://www.dhs.gov/sites/default/files/publications/privacy-piaupdate-tsa-ocims-august2015.pdf.

172 Bogers, 2.

173 Office of the Inspector General, *TSA's Office of Intelligence and Analysis Has Improved Its Field Operations*, 6.

174 Sean M. Hebert, email message to author, June 30, 2021.

partners, etc.[175] Additionally, the TAD intelligence support to the TSA's Global Strategies office helps direct overseas screening efforts and focuses on airports considered higher threats to the transportation sector.[176] The NTVC is a 24/7 unit of watch officers and encounter analysts focused on the vetting and analysis of individuals who may pose a threat to national security and the aviation sector.[177] The Transportation Vetting System (TVS) and Secure Flight, and the Encounter Analysis Branch (EAB), two systems used for vetting reside with the NTVC.[178]

Using the TVS, the TSA conducts forward and recurrent vetting of the credentialed transportation workforce to identify those applicants seeking a transportation credential current credential holders having links to terrorism, or posing other risks to transportation.[179] As an example, the TSA performs continual, recurrent vetting of individuals working within the sterile areas of the airports, who have obtained a TSA Pre-Check privilege, hold FAA credentials, or are crewmembers on a flight.[180] In 2015, the DHS OIG conducted an investigation into the TSA's vetting capabilities, and found that the vetting process was failing.[181] The DHS OIG found that the TSA had provided aviation credentials to 73 individuals with links to terrorism, which happened because the TSA did not have access to all the terrorism-related intelligence the U.S. government maintained.[182] Since the release of the DHS OIG report, it appears the TSA's vetting efforts have proven effective at detecting links to terrorism within the credentialed population. No additional

175 Sean M. Hebert, email message to author, June 30, 2021.

176 Sean M. Hebert, email message to author, June 30, 2021.

177 Wanda Davis, "Wanda (Wanda Frazier) Davis," LinkedIn, August 3, 2019, https://www.linkedin.com/in/wanda-davis-62b350b0/.

178 Office of the Inspector General, *TSA's Office of Intelligence and Analysis Has Improved Its Field Operations*, 6.

179 Office of the Inspector General, *TSA Can Improve Aviation Worker Vetting (Redacted)*, 5.

180 Christina Chesterfield, email message to author, June 12, 2021.

181 Office of the Inspector General, *TSA Can Improve Aviation Worker Vetting (Redacted)*, 2.

182 Office of the Inspector General, 2, 9–11.

reporting indicates the TSA has provided a transportation credential to an individual linked to terrorism.[183]

The TSA's vetting of credentialed employees and applicants supports the IC by keeping individuals with links to today's threats away from secure areas in the transportation network. As an example, after the January 2021 Capitol Hill riots, reported as domestic terrorism, the U.S. Congress urged the TSA to identify all individuals involved in the attack and add them to the federal No-Fly List.[184] Further, the information collected through the vetting process should provide information that the IC can analyze to uncover additional links to foreign and domestic terrorism, insider threats, and TOC activity. For example, a credentialed airline employee hits against the TVS, and initial analysis reveals no derogatory information, but reveals the credentialed individual shares an address with a subject in the TSDB, a KST. Upon further research, DHS data identifies the KST has an active student pilot's license. More research, through FAA data, uncovers the KST is attending a flight school with unknown associates who share a phone number with the KST, as well as the same foreign address listed on their visas. The unknown associates do not appear in any available datasets. At this point, the TSA can provide more information to the IC. This topic is discussed in Chapter V.

Just as valuable is the TSA's Secure Flight program with SP focusing on identifying previously unknown individuals who may pose a higher risk based on their travel patterns and association. QS is also used as an extension of the SP in the domestic realm for the more imminent and critical SP ruleset.[185] Ultimately, "Secure Flight allows TSA and [its] partners in the intelligence community to adapt quickly to new threats."[186] Secure Flight is a powerful and dynamic tool when it comes to terrorist travel. Secure Flight vets fully

---

183 Office of the Inspector General, 9.

184 Bennie G. Thompson, "Chairman Thompson: TSA and FBI Must Add Suspected Domestic Terrorists to No-Fly List and Keep Them off Planes," House Committee on Homeland Security, January 7, 2021, https://homeland.house.gov/news/press-releases/chairman-thompson-tsa-and-fbi-must-add-suspected-domestic-terrorists-to-no-fly-list-and-keep-them-off-planes.

185 Bush, *Privacy Impact Assessment Update for Secure Flight Silent Partner and Quiet Skies*, 1.

186 Steve Sadler, "TSA Secure Flight Program," para. 3, National Security Administration, Secure Flight History, September 18, 2014, https://www.dhs.gov/news/2014/09/18/written-testimony-tsa-house-homeland-security-subcommittee-transportation-security.

known individuals on the TSDB, partially known, or completely unknown higher risk travelers through SP and QS, the internal TSA watchlist for known non-KST subjects, and transportation-related credential vetting to ensure no insider threats.[187] The Secure Flight system is a quick way to identify any subjects who touch TSA equities. Secure Flight data being responded to by the FAMS, such as a KST on a particular flight, is being reported by the FAMS in an AAR.[188] This chapter already noted that the AAR might be serialized, and the information could be used to increase the TSA's intelligence efforts. However, when the FAMS is responding to a Secure Flight match, it can be leveraged for intelligence collection, such as collecting a DNA sample. This topic is discussed in Chapter IV.[189]

The EAB is the last unit within the TSA that plays a critical role in support of the intelligence mission. The EAB is recognized as a DHS IE CIP member. The EAB "identif [ies] potential risks to transportation security by searching for, discovering, and analyzing previously unknown links, trends, or patterns among transportation sector workers and airline passengers."[190] For example, the EAB may discover a credential applicant has provided a unique piece of information (phone number, address, etc.) that associates to an individual in the TSDB. This connected information might warrant further analysis. The EAB works in coordination with the Secure Flight screening of airline passengers, as well as with the data collected through the forward and recurrent vetting of the TVS program. As a result of this analysis, the EAB may identify new information on an individual, or information that reveals an association with a KST, and will either enhance or submit a new watchlist nomination to the terrorist identities database.[191] Depending on the type of information gathered, the EAB may "produce intelligence reports on TSA's encounters with known or suspected terrorist."[192] Both actions, watchlisting and analytical reporting,

---

187 Sean M. Hebert, email message to author, June 30, 2021.

188 Sean M. Hebert, email message to author, June 30, 2021.

189 Mitch Selby, email message to author, June 6, 2021.

190 Matthew Tracey, *Privacy Impact Assessment Update for the TSA Encounter Analysis Branch* (Washington, DC: Department of Homeland Security, 2019), 1, https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsaeab-july2019.pdf.

191 Christina Chesterfield, email message to author, June 12, 2021.

192 Tracey, *Privacy Impact Assessment Update for the TSA Encounter Analysis Branch*, 1–2.

support the IC by providing one more piece of the puzzle and can help identify previously unknown or partially known individuals within the TSA systems.

The research shows that the EAB conducts both strategic and tactical analysis on individuals within the transportation sector. However, the research does not indicate what type of intelligence the EAB uses for analysis, whether DHS only information, or a combination of DHS and IC data. As noted earlier in this chapter, the DHS OIG found that the TSA's vetting of credentialed workers failed in 2015 because the TSA did not have all the IC data available to it. That begs the questions, does the TSA's EAB use IC data in its analysis, and is the EAB still limited in what information it can review? If the EAB had access to a wealth of IC data, the TSA could enhance its intelligence functions through the EAB. The EAB could then conduct strategic analysis on the subjects encountered, to include pattern-of-life analysis, travel pattern analysis (to/from countries of interest), as well as analytic worked based on the FAMS AARs. Further, and just as important, are the EAB's analytic efforts based on national intelligence requirements or internal TSA legacy requirements? If the EAB's analysis is based on non-national priority requirements, then the TSA can enhance its support in this area to the IC. These points are discussed in Chapter V.

Cited literature in this thesis illustrates the TSA's support of U.S. intelligence efforts is focused on tactical and time sensitive operations. However, once executed, it is not clear how the TSA's efforts translate into strategic intelligence that external customers can absorb. While the TSA's watchlisting work does provide enduring analytic input by identifying potential terrorist travel and associations, the TSA can work to increase collection to contribute to an improved IC analysis of potential threats.[193] When viewing the TSA as a whole, and considering its presence both domestically and internationally, it

[193] Tracey, 2.

would be fair to assume the TSA could also collect raw intelligence of value to the U.S. IC and LE communities, albeit with the USPERs' names being redacted.[194]

C. CHAPTER SUMMARY

Unlike the other members of the DHS IE, the TSA was formed in response to a specific act and came into the fold without any historical precedence or guidance. At the time of the TSA's creation, the United States was fearful that another terrorist attack that utilized the aviation sector was possible, and therefore, the United States created the TSA to focus on security within the airports. However, this chapter presented another side of the TSA, with which the public was not familiar. The media rarely reported on this issue. The TSA is more than just the security officers at the airport checking for contraband or odd behavior. The TSA is a national security agency that works to defend against numerous threats.[195] This chapter identified the TSA's current position within the DHS IE, the authorities sustaining the TSA's operational objectives, and the TSA's contribution to the national intelligence mission. The next chapter reviews the existing legal framework that can be used to increase the TSA's support to the IC and the national intelligence cycle.

---

[194] The U.S. IC is limited in the "collection, retention, and dissemination of information concerning unconsenting U.S. persons." IC "minimization procedures generally provide for the substitution of a generic phrase or term, such as 'U.S. person 1' or 'a named U.S. person' when including the identity of the U.S. person does not meet dissemination criteria." As such, the TSA would need to abide by these standards when sharing any U.S. person information with IC or LE partners. Civil Liberties and Privacy Office, *Protecting U.S. Person Identities in Disseminations under the Foreign Intelligence Surveillance Act* (Washington, DC: Office of Director of National Intelligence, 2017), 1–2, https://www.dni.gov/files/documents/icotr/CLPT-USP-Dissemination-Paper---FINAL-clean-11.17.17.pdf.

[195] "Through the end of fiscal year 2016, TSA's behavior detection screening process was a stand-alone program that used specially trained behavior detection officers to observe passengers at the screening checkpoint and engage the in brief verbal exchanges. If the behavior detection officers determined during this interaction that a passenger exhibited a certain number of behavioral indicators, the behavior detection officer was to refer the passenger for additional screening, or if circumstances warranted, contact a law enforcement officer." William Russell, *Aviation Security TSA Has Policies that Prohibit Unlawful Profiling but Should Improve Its Oversight of Behavior Detection Activities*, GAO-19-490T (Washington, DC: Government Accountability Office, 2019), 2, https://www.gao.gov/assets/700/699485.pdf.

IV. LEGAL FRAMEWORK TO ENHANCE THE TSA SUPPORT TO NATIONAL INTELLIGENCE

In 2002, and again in 2006, the USCG and the DEA, respectively, became official members of the U.S. IC.[196] Both entities spent years working together with the IC, and produced valuable intelligence in the ever-present threats that face the United States. The USCG and DEA's transition into the IC was a formalization of their existing performance, but also paved the way to remove organizational obstacles and provide both organizations enhanced access to information on national security.[197] Over the last few years, it has been reported that both the CBP and ICE are working in tandem to petition the ODNI to transition their intelligence units out of the DHS IE and into the IC to become statutory IC members.[198] These entities, like the USCG and DEA, believe they would gain more influence in setting national security priorities, as well as access to the National Intelligence Program (NIP) budget.[199] Such a move may be considered beneficial to CBP and ICE, but such a consideration may not be necessary for the TSA. The TSA may already have the authority to participate in additional intelligence activities without statutory IC membership.

Indeed, as an agency that operates both domestically and overseas, the TSA is situated to provide more value to the nation's intelligence collection, and the IC should make a push to fully leverage TSA's position and access. In this context, the existing laws and directives already address the issue of whether the U.S. government, specifically the

196 Kevin E. Wirth, *The Coast Guard Intelligence Program Enters the Intelligence Community: A Case Study of Congressional Influence on Intelligence Community Evolution* (Washington, DC: National Defense Intelligence College, 2007), 29–30, 52, https://apps.dtic.mil/sti/pdfs/ADA476640.pdf; John D. Negroponte, *Director of National Intelligence* (Washington, DC: Director of National Intelligence, 2006), 1, https://fas.org/irp/dni/dni020706.pdf.

197 Negroponte, 1.

198 Government Technology & Services Coalition's, "CBP, ICE Bids to Join Intelligence Community Gain Traction," Homeland Security Today, 1, February 14, 2018, https://www.hstoday.us/federal-pages/odni/cbp-ice-bids-to-join-intel-community-gain-traction/.

199 Randol, *Department of Homeland Security Intelligence Enterprise*, 7.

IC, can legally expand the TSA's intelligence functions to answer national intelligence priority requirements.[200]

This chapter reviews the existing legal framework with the view of identifying which of its components already validate increasing the TSA's contribution to national intelligence without requiring new legislation. Exploring these authorities and gaining the necessary support from both within and outside the IC will allow the TSA to add valuable intelligence gains for the U.S. government immediately without the need for further legislation.

A. NATIONAL SECURITY ACT OF 1947

To consider expanding the intelligence functions of the TSA, the foundation of the proposal must have merit and be thoughtfully presented to an audience who understands the value of unexplored opportunities. The National Security Act of 1947 (NSA 47), which predates the creation of the TSA, is the foundation of the IC and provides legal merit for enhanced TSA intelligence activity. While NSA 47 does not specifically address the TSA, it does address the capability to enhance the TSA's intelligence functions. First, NSA 47 clearly defines the components of the IC that includes the DHS I&A, which oversees the DHS IE, of which the TSA is a member. This topic was discussed in Chapter III.

This act, in coordination with an agency or department head, such as the TSA Administrator, further states that the President of the United States or the DNI can designate any part of a U.S. agency or department to be a part of the IC.[201] While this thesis is not proposing the TSA become a statutory member of the IC, NSA 47 provides a

---

200 These authorities are derived from the TSA's current position within the DHS, as discussed in Chapter III, the Congressional mandates that established the TSA, and existing laws and directives in place that guide the IC's common framework.

201 National Security Act of 1947, 50 *U.S. Code* 3001 (2018): 5, § 102A et seq., http://www.hlma.net/wp-content/uploads/2018/06/National-Security-Act-Of-1947.pdf. From 1947 until post-9/11, what is now formalized as the DNI, was formerly known as the DCI. During those years, the U.S. IC was sufficiently able to make use of travel information on a case-by-case basis. Since 9/11, the United States has seen an increase in threats as it pertains to the transportation sector, and the creation of the TSA has provided new intelligence collection platforms. The changing threats demand continual changes to the IC. "A Look Back … Directors of Central Intelligence," Central Intelligence Agency, April 30, 2013, https://www.cia.gov/news-information/featured-story-archive/2008-featured-story-archive/directors-of-central-intelligence.html.

contingency to assign IC status to an organization to accommodate national interests.[202] A more likely scenario for the TSA is to rely on this act for legal justification to increase its intelligence programs to support IC members.

As stated in NSA 1947, the DNI is responsible for providing national intelligence to the President, heads of departments and agencies of the executive branch, the Chairman of the Joint Chiefs of Staff and senior military commanders, and the Senate and House of Representatives and the committees. NSA 1947 is also required to provide national intelligence generated from multiple sources and be neutral, politically unbiased, and timely.[203] In line with the DNI's required access to intelligence, NSA 47 states that the DNI must be able to gain access to all national intelligence that has been collected by "any Federal department, agency, or other entity" unless explicitly defined by law.[204] Therefore, NSA 47 clearly does not exclude the TSA from further intelligence participation. The TSA especially has the ability to collect and report on vital national intelligence, such as the actions and intentions of foreign national aviation partners, activities, and associates of domestic terror groups, as well as tracking and reporting on insider threats to the U.S. transportation network.

Additionally, NSA 47 states that the terms "national intelligence" and "intelligence related to national security" describes "all-source" intelligence to all intelligence collected either domestically or overseas.[205] It is fairly easy to envision the TSA supporting additional aspects of the IC and taking advantage of the TSA's large domestic and overseas presence since it is existing member of the DHS IE, with current intelligence collection and analysis capabilities,.

Further, the term "national intelligence program," as stated in NSA 47, includes all activities, plans, and endeavors of the IC, including any other endeavors, with the consent of the President of the United States, or the DNI in coordination with an agency or

---

[202] National Security Act of 1947, 5.

[203] National Security Act of 1947, 9.

[204] National Security Act of 1947, 9.

[205] National Security Act of 1947, 5.

department head.[206] The TSA as a whole does not need to seek statutory IC status, as NSA 47 affords the DNI and the TSA Administrator the ability to designate one or more programs within the TSA with IC authorities and responsibilities.

The initial authorities of NSA 47 have been considerably expanded through 2021 and demonstrate Congress' intent to provide more—not less—authority for the U.S. government, through the DNI, to gain intelligence capabilities.[207] Collectively, the authorities are consistent with Congress' intent and should be read together to provide legal authority for the larger IC to leverage the TSA's intelligence division. The authorities have been delegated by statute to the DNI, which further demonstrates Congress' willingness to allow DHS components to provide the IC expanded collection and analysis platforms in an increasingly challenging security context.[208] The latitude given in this act provided legal justification for the TSA to establish an intelligence platform, such as an overt debriefing program that could be conducted in combination with the TSA's FIOs, the TSA FAMS, and the TSA representatives (TSAR), and be guided and protected by established policies and legislation.[209]

B. EXECUTIVE ORDER 12333

Should the TSA consider expanding its intelligence programs, it is vital that the TSA relies on more than one piece of legislation or policy. This section provides additional justification. Much like NSA 47, EO 12333, issued January 2018, addresses the U.S. intelligence activities, and also provides clear guidance to the DNI, and subordinate department heads. First, EO 12333 stipulates that to acquire insight on any threats toward

206 National Security Act of 1947, 19.

207 National Security Act of 1947, 8.

208 National Security Act of 1947, 12, 18, 21–23, 61–62.

209 The TSAR is "the primary Transportation Security Representative of TSA for foreign governments and embassy officials, ensuring attainment of international security standards, sharing best practices, serving as the on-site coordinator of the TSA/DHS response team to transportation-related terrorist incidents and threats" and among other duties is tasked with "developing stakeholder networks and cultivating effective relationships to manage crisis situations and resolve complex and potentially controversial transportation security issues involving the international community." "Transportation Security Administration Representative (TSAR)," 1, Transportation Security Administration, February 14, 2019, https://diversityjobs.com/jobsearch/display/720379298?utm_medium=social&utm_source=facebook.

the United States, the intelligence must be of the highest quality and have been obtained through appropriate and legal means. The responsibility to analyze and disseminate intelligence falls on each department and agency within the IC.[210] Therefore, the TSA is well positioned to support the IC, which must provide the DNI the highest quality intelligence since the TSA maintains the experts and relationships to report on the transportation sector, either domestically or overseas.

Next, EO 12333 stipulates that in coordination with relevant organizational leaders, the DNI can seek the support of non-IC organizations to engage in the collection and analysis of intelligence pertinent to national security.[211] As written, EO 12333 provides legal cover to enable the TSA to reach further in its collection and analysis of intelligence.[212] The legal cover is consistent with the structure and authorities being used by the DHS CIPs under the DHS IE, as none of the CIPs have IC statutory status, but function under the regulations and laws outlined in EO 12333.[213] Any additional intelligence activities the TSA seeks to conduct should also fall in line with EO 12333.

In addition, EO 12333 stipulates that domestically, the FBI Director is responsible for overseeing all clandestine Human Intelligence (HUMINT) and counterintelligence activity used during foreign intelligence collection. The CIA Director is responsible for overseeing all clandestine HUMINT and counterintelligence activity used during foreign intelligence collection outside of the United States.[214] This stipulation provides another opportunity for the TSA to contribute to the IC's intelligence activity. Indeed, while the TSA would not be legally covered to engage in any type of clandestine activity, as a global

---

210 Reagan, Executive Order 12333, 12.

211 Reagan.

212 Department of Homeland Security, *Requests for Identities of U.S. Persons in Disseminated Intelligence Reports* (Washington, DC: Department of Homeland Security, 2020), 1, https://www.intel.gov/assets/documents/702%20Documents/oversight/DHS_ICPG_107_1_Unmasking_Procedures_022420OCR.pdf.

213 Department of Homeland Security, 1.

214 Reagan, Executive Order 12333. "Human Intelligence (HUMINT). A category of intelligence derived from information collected and provided by human sources." Director of National Intelligence, *Intelligence Community Directive 304—Human Intelligence* (Washington, DC: Office of the Director of National Intelligence, 2009), 6, https://www.dni.gov/files/documents/ICD/ICD%20304.pdf.

entity, the TSA could overtly engage with potential targets of interest. These targets include foreign governments, international air carriers, and foreign airport partnerships that can answer national requirements. The TSA can document and report any known or perceived threats, identify areas of vulnerability, as well as report on targets of potential interest to the IC, such as organizations and individuals. Within the United States, the TSA would fall under the purview and operational guidance of the FBI. Any activity overseas would be under the operational control of the DNI representative, colloquially known as the station chief. Overt collection by the TSA would not seek to impede on either the FBI or CIA's mission, but only act as a force multiplier when natural access to information was necessary, or if transportation intelligence requirements had to be developed in line with traditional national requirements.

In sum, the TSA maintains the experience, expertise, and domestic and foreign relationships in the global transportation network that can support the IC and its mandate to provide the DNI with the highest quality intelligence, through the collection and dissemination of information gathered due to the TSA's position and access. Through EO 12333, the TSA's IC status is irrelevant. The DNI and the TSA Administrator are jointly authorized to use non-IC U.S. government entities in the collection and analysis of intelligence to meet national security demands. The TSA is positioned domestically and overseas to capture information on individuals and organizations linked to overseas terrorism. The TSA can also obtain information on people who may display ideological tendencies to support and engage in domestic terrorism, as well as identify anyone who seeks to cause harm from inside the transportation sector. All this information, if captured and reported in accordance with IC standards, such as the IIR, could provide one more piece to the large puzzle.

C. INTELLIGENCE COMMUNITY DIRECTIVE—900

The legal foundation for the TSA to enhance its intelligence collection and analysis has been set with the two previous pieces of legislation. This section provides the TSA with the best pathway to begin the discussion, on additional intelligence activities, with the appropriate senior leadership. The Intelligence Community Directive—900 (ICD 900) is

an ODNI directive issued in May 2013 that outlines integrated mission management. ICD 900 receives its authority from the following regulations: NSA 47, IRTPA, and EO 12333.[215] ICD 900 introduces the role of the national intelligence managers (NIMs), who provide the DNI with advice regarding strategic and tactical intelligence pertaining to a NIM's portfolio, such as a region of the world, or a topic or function.[216] For example, the National Counterterrorism Center is a functional NIM, whereas the National Intelligence Manager—Aviation (NIM-A) is a topical NIM.[217] The NIM-A is responsible for all intelligence related to aviation, to include the aviation ecosystem, as introduced in Chapter I. The TSA should seek out the NIM-A's support to receive guidance and direction to expand its role.

ICD 900 also provides guidance the NIMs should follow to attain agreement seamlessly on their efforts and impacts regarding intelligence missions. The guidelines within ICD 900 stipulate managing the integration of cross-domain intelligence to achieve unity among the NIM's areas or topics of operations, the alignment of intelligence disciplines, as well as integrating the production, processes, and activities of intelligence.[218] In this connection, the TSA is mandated through the ATSA to "receive, assess, and distribute" all relevant intelligence related to transportation security by recognizing the relationship between the TSA's intelligence division and the NIM-A's responsibility to integrate all intelligence activities in the domain. A joint decision by the DNI and NIM-A would result in support from members of the IC to take advantage of the TSA's ability to garner more transportation intelligence responding to national requirements.[219]

---

[215] Director of National Intelligence, *Intelligence Community Directive 900—Integrated Mission Management* (Washington, DC: Office of the Director of National Intelligence, 2013), 1, https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives.

[216] Director of National Intelligence, 2.

[217] "Organization," 1, Office of the Director of National Intelligence, accessed April 25, 2019, https://www.odni.gov/index.php/component/content/article?id=341&Itemid=583.

[218] Director of National Intelligence, *Intelligence Community Directive 900*, 3.

[219] Aviation and Transportation Security Act of 2001, 2.

For example, the FBI notifies the TSA that an individual, previously unknown to have domestic extremism links, will be boarding a domestic flight in the next few hours. The FBI is requesting support from the TSA FAMS to collect a biological sample, such as DNA, while on the plane with the subject.[220] In this scenario, the DNI and NIM-A agreed to enhance the TSA's intelligence footprint, with the TSA FAMS having been provided with specialized training, funded through the NIP, to collect and report on such operational instances. The FAMS collects the sample, passes it off to the FBI for processing, and then submits an IIR for IC dissemination. The inclusion of the IIR into IC holdings pieces together biographical and assessment data on the subject, and identifies associates of the subject, and some of the subject's associates working within the credentialed transportation sector.

Ultimately, then, just like NSA 47 and EO 12333, ICD 900 is provided for the IC's guidance, but also to any U.S. government entity the President of the United States, or the DNI in coordination with an agency or department head, such as the TSA Administrator, sees fit to provide such a designation.[221] The TSA, as noted in the example, would then be able to participate legally in activities previously not considered a function of TSA intelligence personnel, but also in situations in which the TSA would have a more natural approach to provide greater benefits to the safety of the United States.

D. INTELLIGENCE COMMUNITY DIRECTIVE—204

It is not enough for the TSA to know it can legally increase its contribution to the IC, or that it will need the support of, in addition to the DNI and the TSA Administrator, the NIM-A. The TSA's participation in additional intelligence activities can be bolstered through the development of transportation intelligence requirements, which will

---

[220] Anthony Kimery, "DNA Processing Carried Out by DHS S&T for FBI, Intel Agencies," Biometric Update, January 14, 2019, https://www.biometricupdate.com/201901/dna-processing-carried-out-by-dhs-st-for-fbi-intel-agencies. It is not illegal to collect the human Deoxyribonucleic acid (hDNA) that has been considered abandoned, unless by coercion. The collection of an hDNA sample that has been abandoned is not protected under the U.S. Fourth Amendment. Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, vol. 100, no. 2 (Chicago: Northwestern University Law Review, 2006), 859, http://www.antoniocasella.eu/dnlaw/Joh_2006.pdf.

[221] Director of National Intelligence, *Intelligence Community Directive 900*, 1.

distinguish the TSA from the rest of the DHS IE and align itself with the standards of the IC. The Intelligence Community Directive—204 (ICD 204) is an ODNI directive re-issued in January 2021, which outlines the NIPF.[222] ICD 204 receives its authority from the following regulations: NSA 47, IRTPA, EO 12333, and the National Security Presidential Directive-26, Intelligence Priorities.[223] ICD 204 is not a directive that provides legal authority for the TSA to engage in intelligence activities, but a directive that provides the structure in which the nation's intelligence priorities are ordered, how the priorities can be interpreted for action, and the assessment of how the IC responds to the priorities.[224]

Further, ICD 204 defines the NIM-A's role to advise the DNI on the creation of national intelligence priorities, to include intelligence needs and intelligence gaps, as well as ad-hoc priorities for emergent intelligence needs.[225] These priorities are specific to the NIM-A's area of operation. For example, the TSA Administrator may possibly recognize a gap in the intelligence that either the DHS or IC is not collecting regarding the aviation ecosystem and then determine that collection needs to occur. The TSA Administrator can provide the intelligence priorities to the NIM-A, who in turn, advises the DNI on these intelligence gaps. Additionally, just as the legislations and directive noted earlier, ICD 204 is also applicable to non-IC U.S. government entities, when designated by the President of the United States, or the DNI in coordination with an agency or department head. The TSA can then use ICD 204 as a roadmap to implement intelligence priorities specific to the TSA's mission.[226]

For the TSA, as an intelligence element within the DHS I&A, intelligence priorities are a necessity to direct TSA resources pertaining to intelligence collection. Intelligence priorities serve as a guidepost to show the TSA where it has collected intelligence, where

---

[222] Director of National Intelligence, *Intelligence Community Directive 204—National Intelligence Priorities Framework* (Washington, DC: Office of the Director of National Intelligence, 2021), 1, https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf.

[223] Director of National Intelligence, 1.

[224] Director of National Intelligence, 1.

[225] Director of National Intelligence, 3–4.

[226] Director of National Intelligence, 1.

the intelligence gaps exist, and where the TSA needs to focus its collection efforts. Chapter III revealed that the DHS I&A released a Strategic Plan for Fiscal Year 2011–2018 that included the HSIPF, ostensibly to guide the DHS I&A intelligence collection efforts. However, a June 2014 GAO report found that while the DHS maintained an intelligence framework, the framework came up short by not setting strategic level intelligence priorities for the department.[227] Additionally, the 2020 UDHSIC Act came up short by not introducing intelligence priorities. Between the 2011 Strategic Plan and the UDHSIC Act, it appears the DHS has not implemented an intelligence priority framework either at the department level or for the DHS CIP units. If the DHS has implemented a framework, the research does not show it being directed, or even marketed to the DHS IE. Not incorporating such measures, especially after 19 years, separates DHS intelligence from the rest of the IC.

In discussing the distinction between the national intelligence community and the homeland IE in 2016, Todd Rosenblum, former Acting Assistant Secretary of Defense for Homeland Defense and America's Security Affairs (2013–2015), noted the work of the DHS IE amounts to "investigative data supporting tactical operations, not the strategic, predictive work that is the bread and butter of the IC."[228] In discussing the limits and capabilities of the homeland IE, Mr. Rosenblum believes the DHS IE needs to develop "intelligence tradecraft, the dissemination of finished intelligence and broader collaboration."[229]

The lack of an enterprise-wide framework to guide intelligence collection puts the TSA at a disadvantage. Notwithstanding, the research identified Ms. Stacey Fitzmaurice, while serving as the Deputy Assistant Administrator for the TSA's Intelligence & Analysis (I&A) office (2015–2016), was charged, among other initiatives, to create the first

---

227 Government Accountability Office, *DHS Intelligence Analysis*, 3–4, 12, 40.

228 Todd Rosenblum, "Homeland Intelligence: The Unique Community within the Community," *The Cipher Brief* (blog), 1, October 9, 2016, https://www.thecipherbrief.com/column_article/homeland-intelligence-the-unique-community-within-the-community.

229 Rosenblum, 1.

intelligence priorities for the TSA I&A office.[230] However, these requirements appear to be localized to the office level and potentially focused on the TSA's tactical or transactional mission set.[231] The effort made by Ms. Fitzmaurice showed that the TSA, at least at the office level, recognized the importance of establishing intelligence priorities.

Both CBP and ICE, for example, have made efforts to become statutory IC members in essence to have more authoritative input into shaping the NIPF.[232] However, the TSA, in coordination with the NIM-A, could achieve similar results as sought by CBP and ICE with existing legislation and directives. ICD 204 provides a path for the TSA, in coordination with the NIM-A's input into the NIPF, the ability to gain more influence in setting national security priorities, specifically as they relate to transportation intelligence.

Overall, the TSA could position itself much like the Armed Forces Service IC components, by primarily responding to requirements that answer the needs of the TSA, while contributing to the larger IC body of knowledge.

E. CHAPTER SUMMARY

This chapter provided the current laws and directives that could be considered to justify the legal authority for the U.S. government, specifically the IC, to look deeper into expanding the TSA's intelligence capabilities as a non-statutory IC member.

The research found that these authorities allowed the TSA to participate in additional intelligence activities usually associated with statutory IC members. By way of the NIM-A, the TSA could begin to establish national intelligence priorities that not only answered intelligence gaps in the U.S. transportation sector but also supported the larger IC requirements. In this manner, the TSA will augment the IC's readiness to meet the White House's requirement to protect the aviation ecosystem through an all-inclusive and compatible approach beyond FTOs and impede the domestic terrorist, insider threat, TOCs,

230 "Operations Support—Executive Assistant Administrator," 1, Transportation Security Administration, accessed July 5, 2021, https://www.tsa.gov/leader-bios/operations-support.

231 Transportation Security Administration.

232 Government Technology & Services Coalition's, "CBP, ICE Bids."

and foreign intelligence activity.[233] Any effort to do so cannot solely occur internal to the agency, as within a vacuum. All efforts to leverage the TSA's capabilities and global reach must be developed with the cooperation of multiple departments and agencies, and use the current laws, acts, and directives available.

The next chapter provides findings and recommendations to enhance the TSA's support to intelligence, with consideration for how the IC can support and leverage the TSA's IC capabilities. Finally, Chapter V presents a conclusion and proposes future research.

233 Trump, *National Strategy for Aviation Security of the United States of America*, 7–17.

V. FINDINGS, RECOMMENDATIONS, AND CONCLUSION

This thesis described how the U.S. IC could more effectively leverage the TSA's position and access to valuable information to improve the security of the United States. To this end, it first broke down the current threats facing America 20 years after the AQ attacks on 9/11, followed by TSA's operational activities, and its current role supporting U.S. national intelligence. This thesis then explored the legislation to justify increasing the TSA's contribution to national intelligence. This chapter first provides the findings of this research, followed by recommendations for decision makers to consider should they wish to develop the TSA's continued support to national security further, and addresses potential sources of funding to support the recommendations. The chapter ends with a future research recommendation and a conclusion.

A. FINDINGS

This thesis found that FTOs were no longer the most significant threat to U.S. national security, and that the United States was facing a wide range of threats from domestic terrorists, transnational organized criminals, and espionage from both overseas actors and those in the homeland.[234] Additionally, this thesis found in Chapter III that the TSA must continually evolve to respond to the emerging threats on the aviation ecosystem and the entire U.S. transportation sector.

Further, this thesis found that the TSA was already providing occasional valuable intelligence to the IC and LE communities. The TSA nevertheless can provide more value to the IC through advanced intelligence collection, dissemination of raw intelligence, as well as preparing strategic analytic products. Finally, this thesis found that existing legislation would allow the TSA to participate legally in additional intelligence gathering activities in support of the U.S. IC.

234 Transportation Security Act of 2001.

B. RECOMMENDATIONS TO ENHANCE THE TSA'S SUPPORT TO INTELLIGENCE

In line with these findings, this thesis proposes the following recommendations: develop specific transportation intelligence requirements, establish a collection management program, modernize the TSA's intelligence functions, and establish a TSA overt strategic debriefing program.

1. Develop Specific Transportation Intelligence Requirements

The first recommendation is for the IC to develop specific transportation intelligence requirements. As explained in Chapter IV, the TSA could participate in additional intelligence activities by developing transportation intelligence requirements unique to the TSA and aligned with IC standards, specifically the NIPF.[235] Further, Chapter IV pointed out that the DHS had not yet implemented an intelligence priority framework that the members of the DHS CIPs could follow. With the creation and inclusion of transportation intelligence requirements, the TSA would have a definitive roadmap for intelligence activities.[236]

The TSA should involve itself, in coordination with the NIM-A, in the development of requirements for the NIPF based on the TSA's extensive knowledge and experience in the transportation sector. Additionally, the TSA should actively provide the NIM-A with intelligence gaps not being collected from the IC. An example in Chapter IV illustrates the TSA Administrator's need for intelligence on the aviation ecosystem when collection has not occurred. The TSA's involvement with forming national priorities will elevate the value of transportation intelligence requirements for both the TSA and other IC members. As the national priorities are a formal communication of the President's priorities regarding national security, agencies external to the TSA will regard transportation intelligence requirements as valid and attempt to collect against such requirements.

---

[235] Director of National Intelligence, *Intelligence Community Directive 204*.

[236] Rosenblum, "Homeland Intelligence."

For the TSA to outline intelligence priorities, which will guide its collection efforts, it will need to review the threats from Chapter I. The TSA management will then need to analyze its current organizational structure and capabilities against those threats in Chapter III to align the appropriate operational resources. The TSA should consider how the threats from Chapter I can be more effectively mitigated in the operational spaces the TSA occupies, to include the airports, airplanes, cargo facilities, and all surface transportation.

The national intelligence priorities are ranked from high to low. Multiple U.S. government agencies are already collecting on the emerging threats and focusing on the higher-level hard targets that receive constant attention from policy makers. The TSA should not shy away from these collection efforts but should develop its priorities on these types of targets with a niche focus. This focus could include TOC activity using American transportation networks overseas, or individuals who align with domestic terrorist organizations, specifically individuals who maintain TSA credentials to work in the transportation sector. According to Chapter III, while no legislation currently addresses the domestic terrorism threat, the TSA remains responsible for the protection of the transportation sector. In this way, the TSA should not be collecting on another agency's area of expertise. The TSA's intelligence collection should supplement said agency's national security efforts.

Just as the IC has continued to shift away from counterterrorism collection and analysis as the main national priority requirement, the TSA should take an all-inclusive approach to its long-term intelligence contributions by establishing national transportation intelligence requirements to be listed in the NIPF. Further, the TSA will need to introduce the national intelligence cycle to the workforce through training and education modeled on existing intelligence coursework from external agencies. In doing so, the TSA will be able to respond to threats that have an impact on the U.S. transportation sector and will lead the TSA to optimize its resources and evolve the organization in support of U.S. national security.

2. Establish a Collection Management Program

The second recommendation is to establish a collection management program at the TSA. Tackling the threats to the U.S. transportation sector will require the talent and perspectives from within multiple TSA offices. Integrating the expertise of the TSA offices into a cross-functional intelligence program would require a robust management of knowledge and available resources and assets.[237] In Chapter III, this thesis identified that the TSA already maintained access to the resources and assets required for a successful collection management program, to include information technology (such as WebEOC) and personnel. These resources and assets however are dispersed within the agency.

Therefore, the TSA will want to localize the collection management role within the cross-functional program. The role of a Collection Management Officer (CMO) is the focal point between the TSA and the U.S. policy makers. CMOs are responsible for driving the collection of intelligence and evaluating the intelligence the TSA collects to ensure the appropriate decision makers have well-timed, precise, and succinct reporting. To illustrate, the TSA CMO will engage with senior policy makers to understand the tactical and strategic needs. The TSA CMO will also direct the collection activities of the FIOs, FAMs, and TSARs and guide each to stay on track with current intelligence collection and reporting requirements. To this end, collection management will allow for quickly accessing valuable information and can "provide invaluable insight into how each component of an intelligence operation is functioning or performing."[238] Through a robust collection management program, the TSA should be able to determine its most valuable collection sources and identify gaps for collection needs, which further adds to the continual development and refinement of TSA intelligence priorities.

---

[237] The available literature does not identify whether the TSA incorporates a collection management program for its intelligence functions. However, whether an organization is matrixed, functional, divisional, or flat, the foundation for healthy knowledge management and source validation begins with collection management.

[238] Flashpoint, "Oversight of Intelligence Operations Begins with Collections Management," *Flashpoint* (blog), 1, September 27, 2018, https://www.flashpoint-intel.com/blog/oversight-of-intelligence-operations-begins-with-collections-management/.

If it does not already have an established collection management program, the TSA should consider establishing one in line with the IC as a foundation before making any future enhancements to its intelligence collection. This alignment may not necessarily function or be as robust as other collection management programs in the IC since the TSA's mission set and authorities are not the same. According to a recent CIA CMO job description, a collection manager should have a "combination of formal training and independent learning," and have "subject matter expertise," which includes a focus on "region-specific issues and/or transnational issues such as counterterrorism," as well as on insider threat issues.[239] Therefore, the TSA will want to consider these experiences when filling the collection management roles. The TSA also needs to consider individuals with a strong background in the U.S. transportation sector, such as an intelligence analyst or an experienced FAMS officer with knowledge of working intelligence operations. These individuals must be able to think critically, to communicate effectively verbally and in writing, and understand the TSA's intelligence requirements.

Collection management is used to interpret intelligence requirements into tactical or strategic operational objectives and directs those collecting information and analyzing the collected information.[240] For the TSA to have a functioning collection management program to allow it to identify areas in which it can support national security, it will need to not only receive, but also provide input into the national strategy when this input relates to the U.S. transportation sector. This strategy is the baseline for intelligence requirements that "reflect consideration of the value of intelligence activities."[241]

3. Modernize the TSA's Intelligence Functions

The third recommendation is to modernize the TSA's intelligence functions. No organization can function at the highest level or provide a superior product if it is not continually improved. In 2015, the CIA made significant changes to its approach by adding

239 "Collection Management Officer," Central Intelligence Agency, 1, August 6, 2018, https://www.cia.gov/careers/jobs/collection-management-officer/.

240 Franz, "Beyond Desert Storm."

241 Director of National Intelligence, *Intelligence Community Directive 204*, 2.

a new directorate, as well as establishing 10 new mission centers to be "fully optimized to meet current and future challenges."[242] While the CIA has an extensive mission set and has had more time to refine its organizational structure than the TSA, correlations exist between the two agencies. If mimicked on a smaller scale, the TSA can improve its intelligence processes, which will eventually lead to more intelligence gains since it relates to protecting the U.S. transportation sector. Optimizing the TSA would include streamlining the expertise of multiple offices and divisions into cross-functional teams, such as the CIA's mission centers.

According to Chapter IV, the TSA should consider streamlining its intelligence functions by setting up cross-functional teams from each division that would include expertise in intelligence, law enforcement, tactical (transactional) and strategic objectives, human capital, technical, and analytic support, and align the teams according to the TSA's intelligence priorities framework. For example, cross-functional teams could be structured by topic or region. Teams could then be focused on aviation in one regional area, or teams focused on all transportation nodes in a regional area. By modernizing the organization with cross-functional teams, the TSA could gain a better understanding of its intelligence value, through the input of staff members who maintain diverse viewpoints and experiences. This organizational and systematic change could allow the TSA to be more effectively in line to address the *Air Domain Surveillance and Intelligence Integration Plan*. That plan recognizes the "threats in the [Aviation Ecosystem] are continually evolving and require constant monitoring and adjustments in methods for collecting, analyzing…intelligence, and other information."[243] Further, a diverse team focusing on the TSA's intelligence functions could be able to engage in current operations and identify potential gaps. For example, which intelligence priorities requiring the most attention could be filled with a previously discussed collection management program?

---

242 "CIA Achieves Key Milestone in Agency-Wide Modernization Initiative," 1, Central Intelligence Agency, October 1, 2015, https://intelligencecommunitynews.com/cia-achieves-key-milestone-in-agency-wide-modernization-initiative/.

243 Department of Homeland Security, *Air Domain Surveillance and Intelligence Integration Plan* (Washington, DC: United States Department of Defense, Office of the Secretary of Defense, Office of the Director of National Intelligence, 2007), 3, https://www.hsdl.org/?view&did=472112.

Chapter III laid out the structure of the TSA's I&A office, which included its field mission through its FIOs, multiple 24/7 watch floors, and the EAB within the TSA's NTVC.[244] All these units play a role in intelligence collection to contribute to improved IC analysis of potential threats to U.S. national security. However, implementing these previously discussed cross-functional teams could allow the TSA to incorporate the expertise of units outside I&A. These units include the Law Enforcement/Federal Air Marshal Service, Security Operations, and Enterprise Support, among others.[245] In Chapter IV, the DHS intelligence products were described as "investigative data supporting tactical operations," which had been limiting the DHS's intelligence contributions.[246] Therefore, to not restrict the capabilities of the TSA, the TSA should develop a plan to leverage the experience and expertise of its offices to optimize its intelligence collection to support strategic objectives.[247]

4. Establish a TSA Overt Strategic Debriefing Program

The fourth recommendation is to develop a TSA overt strategic debriefing program. Indeed, after successfully implementing the three previous recommendations, the TSA, using its existing organizational assets described in Chapter III, could increase its intelligence functions to respond to the threats from Chapter I to support national intelligence. To this end, the TSA should consider establishing an overt strategic debriefing program that takes advantage of both its domestic and international presence. Such a program would be responsible for developing and executing overt HUMINT collection operations to include intelligence debriefings of overt sources, drafting raw intelligence reports, responding to customer requests for intelligence and collection management requirements, as well as maintaining detailed operational records.

---

244 Department of Homeland Security Office of the Inspector General, *TSA's Office of Intelligence and Analysis Has Improved Its Field Operations* (Washington, DC: Department of Homeland Security Office of the Inspector General, 2017), https://www.oversight.gov/report/dhs/tsas-office-intelligence-and-analysis-has-improved-its-field-operations.

245 "Leadership and Organization," Transportation Security Administration, accessed July 5, 2021, https://www.tsa.gov/about/tsa-leadership.

246 Rosenblum, "Homeland Intelligence," 1.

247 Rosenblum.

The TSA already has an existing structure for this type of intelligence activity with the current placement of the FIOs and FAMS from Chapter III, as well as with the TSA's internationally placed TSARs who work out of U.S. embassies. The TSA currently engages in potentially reportable interactions with foreign partners, through foreign airport assessments and carrier inspections, as well as the TSA's audits of foreign repair stations.[248] Both the FIO's and the TSAR's baseline positions should be about forming relationships with individuals and organizations with ties to the transportation sector.[249] Both these positions lend themselves for consideration of an overt debriefing program that may answer priority NIPF transportation requirements. These requirements should be reported in a standard intelligence format, such as the IIR. The TSA overt strategic debriefer would not be recruiting sources, such as a CIA operations officer, but would interview TSA and DHS staff who had collected information in the course of their official U.S. government duties.[250]

The TSA and DHS encompass thousands of employees who travel and engage with targets of interest to the IC. Some of these interactions will answer NIPF requirements and can be documented by the FIOs, FAMS, or TSARs for dissemination to the IC for analysis. As discussed in Chapter III, any information shared with the IC would mask the name of the USPER providing the information. To address the TSA's large footprint, the TSA will want to consider how the debriefers are situated within its organization. The TSA debriefers could be headquarters based and deployed to certain domestic or international locations for a specified period, or the debriefers could receive a permanent change of station to a location away from headquarters.

Further, the TSA FIOs could be deployed in both domestic and foreign airports, preferably in countries that did not have a TSAR to engage with individuals with positions

---

248 H.R., *Examining TSA's Global Efforts*, 3.

249 Transportation Security Administration, "Transportation Security Administration Representative (TSAR)."

250 CIA operations officers "clandestinely spot, assess, develop, recruit, and handle non-U.S. citizens with access to foreign intelligence vital to U.S. foreign policy and national security decision-makers." "Operations Officer—CIA," Central Intelligence Agency, accessed July 31, 2021, https://www.cia.gov/careers/jobs/operations-officer/.

and access to answer transportation priority requirements. The FIOs and TSARs would debrief foreign nationals within the transportation sector able to respond to the priority requirements. The FIOs and TSARs would also debrief DHS employees who had traveled overseas representing the U.S. government, and interacted with foreign nationals, foreign organizations, or foreign facilities who might be able to respond to the intelligence requirements.[251] The initial reaction to such a proposal may seem far-fetched and be met with resistance, such as the public's fear of government overreach, or the presses' and Congresses' beliefs from Chapter II that the TSA should be privatized. However, such hesitation can be abated by recognizing that strategic debriefing only engages with people willing to answer intelligence requirements. Such meetings with voluntary participants must be non-aggressive and professional in nature.[252] As noted in Chapter IV, the TSA would not be allowed to engage in clandestine activity since all collection activity would be overt in nature.

The situation becomes much more difficult when considering strategic debriefing, which the IC may attribute to HUMINT. Areas to consider are the recruitment of HUMINT collectors to the TSA, if the TSA does not want to use the FIOs in place, or simply needs to add more collectors to meet demand. Additionally, the TSA must consider how the debriefers will be trained. While this thesis does propose the current FIOs can conduct the debriefing mission, TSA's human capital (HC) will recognize that new recruits without training will always be in the pipeline. Therefore, the TSA will want to determine if it wants to train debriefers from its standards, or if it will choose to use an existing training course that may be provided by one or more IC members.

Chapter IV briefly discussed these training questions that the TSA would face, in the example of the FBI seeking the assistance of the FAMS in the collection of valuable

---

[251] Such activity is not uncommon, as the DOD uses debriefing techniques at both the tactical and strategic level to engage "emigres, refugees, displaced persons, defectors, and selected U.S. personnel." Department of the Army, *Human Intelligence Collector Operations*, 84.

[252] Department of the Army, 16, 84, 108.

information, such as human DNA.[253] With the support of the external IC agencies and their funding mechanisms, specifically the NIP, the TSA should consider using the existing training systems in place for both new collector training, as well as identifying existing personnel with collection training and experience; no need to reinvent the wheel. Also, given the high-paced HUMINT collection efforts over the last 20 years, in various operating environments, it would seem probable that many viable candidates could fill the TSA collection pipeline for years to come and ease potential concerns for the TSA HC and the TSA's senior leadership.

Finally, and while not necessarily an immediate debate, will the TSA want to consider whether its debriefers are allowed to work in a joint-duty assignment with another IC organization, ostensibly to conduct activity in a debriefer capacity? Given that the TSA overt strategic debriefer position will be a new career path for the agency, those who want to compete for such positions will be interested to know what type of professional growth they may experience. Allowing the TSA debriefers the ability to conduct a join-duty assignment will be at the discretion of the TSA senior leadership and the TSA HC. Allowing a TSA debriefer however the capability to experience the operational activity of an external agency can prove valuable. First, the TSA debriefer will potentially gain experience with an organization that has been conducting overt HUMINT activity for decades, and in all types of operational environments. This type of experience will be of value to both newly trained debriefers, and seasoned debriefers alike. Most importantly, the returning joint-duty TSA debriefers will return to the TSA with a wealth of knowledge and should have the proficiency to pass along their experience to the TSA to grow and mature its newly functioning intelligence capability.

[253] As noted in Chapter IV, the collection of hDNA is not illegal. hDNA, which has been identified to a specific individual, may be collected if the hDNA sample has been determined abandoned, such as, for example, a plastic soda bottle left at a public dining table may be collected legally if the person associated with that bottle has clearly left the item behind. The collection of the hDNA is acceptable if it is not collected under coercion. Many articles, journals, and legal rulings discuss the collection of hDNA, and collection efforts to obtain a person's DNA should not be considered a nefarious act. The collection of abandoned hDNA may be surprising to the general public. The general public's knowledge of the possible hDNA collection by the TSA would need to be addressed in the paradigm of continued security to the transportation sector.

5. Funding the Implementation of the Recommendations

Overall, reporting on information of intelligence value, through overt strategic debriefing, is a prudent measure considering the shifting focus of national priorities.[254] While HC and budget restraints are a reality for most U.S. government organizations, the TSA does not have to start from scratch. The TSA can begin with the training and experience of existing intelligence programs, and potentially access funds from the NIP budget from Chapter IV.[255] Not only is the NIP budget flexible to move programmed money into different operational requirements, but the NIP funding can be used by non-statutory IC elements of the U.S. government from Chapter IV.[256] This type of effort will allow the TSA to optimize itself in today's current threat environment and provide enhanced support to U.S. national security.

C. CONCLUSION AND FUTURE RESEARCH

This thesis proposes consideration should be given to leverage further the collection of systems, policies, and procedures of the DHS to counter today's threats more fully. While multiple components of the DHS contribute to the U.S. intelligence cycle, this thesis focuses on the value of the TSA's contributions to lay the groundwork to illustrate the TSA's advantageous position to collect and report on priority intelligence requirements.[257]

Research revealed that the TSA was uniquely situated to capitalize on the organization's existing structure for additional intelligence gains. With some adjustments to processes, personnel, and policy considerations, the TSA could grow from its initial directive of aviation security to its full legal design, as stated by the U.S. Congress to "develop policies, strategies, and plans for dealing with threats," and "make other plans

254 Swan, "DHS Looking at Tracking Travel of Domestic Extremists."

255 "HUMINT," Defense Intelligence Agency, accessed December 17, 2020, https://www.dia.mil/Careers-Internships/Career-Fields/Human-Intelligence/#overview.

256 The NIP is divided into three programs: civilian, defense, and community wide. Included within the NIP's civilian program is the DHS Program, in which the DNI can transfer or reprogram "5 percent of any NIP funds for an agency." Lowenthal, *Intelligence*.

257 Department of Homeland Security, "The Intelligence Enterprise," 11–12, 20.

related to transportation security, including coordinating countermeasures" in support of U.S. national security.[258]

As noted in Chapter III, the intelligence being produced within the DHS had been compared to spam. With the implementation of the thesis recommendations, the DHS, and more specifically, the TSA's intelligence, can move to the proverbial "Inbox."

The next research focus could be the cost-benefit analysis to implement the thesis' recommendations. Future research could be useful in determining the economical pros and cons of the thesis proposal and identify any alternate budgetary proposal that might need to be considered.

[258] Aviation and Transportation Security Act of 2001, 2.

LIST OF REFERENCES

Aaronson, Trevor. "Terrorism's Double Standard: Violent Far-Right Extremists Are Rarely Prosecuted as Terrorists." The Intercept, March 23, 2019. https://theintercept.com/2019/03/23/domestic-terrorism-fbi-prosecutions/.

Adamczyk, Christopher J. "Gods versus Titans: Ideological Indicators of Identitarian Violence." Master's thesis, Naval Postgraduate School, 2020. https://www.hsdl.org/?abstract&did=847107.

American Civil Liberties Union. "How the USA PATRIOT Act Redefines 'Domestic Terrorism.'" Accessed June 14, 2021. https://www.aclu.org/other/how-usa-patriot-act-redefines-domestic-terrorism.

Anti-Defamation League. "The Boogaloo Movement." Accessed June 14, 2021. https://www.adl.org/boogaloo.

Barth, Bradley, and Teri Robinson. "Former CIA Director Brennan Recounts His Transformation into a Full-Fledged Cyber Strategist." SC Media, October 10, 2018. https://www.scmagazine.com/news/-/former-cia-director-brennan-recounts-his-transformation-into-a-full-fledged-cyber-strategist.

Bean, Brian. "Mitigating Insider Threats in the Domestic Aviation System: Policy Options for TSA." *Homeland Security Affairs* (blog). December 1, 2017. https://www.hsaj.org/articles/14380.

Becker, Andrew. "Lawmaker Says TSA Should Focus on Intelligence, Get Out of Screening." Reveal from The Center for Investigative Reporting, April 28, 2016. https://www.revealnews.org/blog/lawmaker-says-tsa-should-focus-on-intelligence-get-out-of-screening/.

Becker, Andrew, and G. W. Schulz. "Homeland Security Office Creates 'Intelligence Spam,' Insiders Claim." Reveal from The Center for Investigative Reporting, November 30, 2011. https://www.revealnews.org/article/homeland-security-office-creates-intelligence-spam-insiders-claim/.

Bergen, Peter, Albert Ford, Alyssa Sims, and David Sterman. "Part IV. What Is the Threat to the United States Today?." New America, 2021. http://newamerica.org/in-depth/terrorism-in-america/what-threat-united-states-today/.

Bogers, John. *Privacy Impact Assessment Update for the TSA Operations Center Incident Management System*. Washington, DC: Department of Homeland Security, 2015. https://www.dhs.gov/sites/default/files/publications/privacy-piaupdate-tsa-ocims-august2015.pdf.

Burch, James. “The Domestic Intelligence Gap: Progress since 9/11?.” *Homeland Security Affairs* XVII (April 1, 2008). https://www.hsaj.org/articles/129.

Bush, George W. *Homeland Presidential Security Directive 6—Directive on Integration and Use of Screening Information to Protect against Terrorism*. Washington, DC: U.S. Government Publishing Office, 2003. https://www.govinfo.gov/content/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1174.pdf.

———. *National Strategy for Homeland Security*. Washington, DC: White House, 2002. https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf.

Bush, Thomas. *Privacy Impact Assessment Update for Secure Flight*. Washington, DC: Department of Homeland Security, 2017. https://www.dhs.gov/sites/default/files/publications/pia_tsa_secureflight_18%28h%29_july2017.pdf.

———. *Privacy Impact Assessment Update for Secure Flight Silent Partner and Quiet Skies*. Washington, DC: Department of Homeland Security, 2019. https://www.dhs.gov/sites/default/files/publications/pia-tsa-spqs018i-april2019_1.pdf.

Central Intelligence Agency. “CIA Achieves Key Milestone in Agency-Wide Modernization Initiative.” October 1, 2015. https://intelligencecommunitynews.com/cia-achieves-key-milestone-in-agency-wide-modernization-initiative/.

———. “Collection Management Officer.” August 6, 2018. https://www.cia.gov/careers/jobs/collection-management-officer/.

———. “Directors of Central Intelligence.” April 30, 2013. https://www.cia.gov/news-information/featured-story-archive/2008-featured-story-archive/directors-of-central-intelligence.html.

———. “Operations Officer—CIA.” Accessed July 31, 2021. https://www.cia.gov/careers/jobs/operations-officer/.

Civil Liberties and Privacy Office. *Protecting U.S. Person Identities in Disseminations under the Foreign Intelligence Surveillance Act*. Washington, DC: Office of Director of National Intelligence, 2017. https://www.dni.gov/files/documents/icotr/CLPT-USP-Dissemination-Paper---FINAL-clean-11.17.17.pdf.

Coats, Daniel R. *DNI Coats Opening Statement on the 2019 Worldwide Threat Assessment of the U.S. Intelligence Community*. Washington, DC: Office of the Director of National Intelligence, 2019. https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1949-dni-coats-opening-statement-on-the-2019-worldwide-threat-assessment-of-the-us-intelligence-community.

———. *National Intelligence Strategy of the United States of America*. Washington, DC: Office of the Director of National Intelligence, 2019. https://www.dni.gov/index.php/newsroom/reports-publications/item/1943-2019-national-intelligence-strategy.

———. *Worldwide Threat Assessment of the U.S. Intelligence Community*. Washington, DC: Office of the Director of National Intelligence, 2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

Cogswell, Patricia F. S. "Protecting the Nation's Transportation Systems: Oversight of the Transportation Security Administration." Transportation Security Administration, September 11, 2019. https://www.tsa.gov/news/press/testimony/2019/09/11/protecting-nations-transportation-systems-oversight-transportation.

Cohen, Jesse. "Securing the Air Cargo Supply Chain." Freight Waves, April 17, 2019. https://www.freightwaves.com/news/airfreight/securing-the-air-cargo-supply-chain.

Crawford, Neta C. *Costs of War*. Providence, RI: Brown University, Watson Institute International and Public Affairs, 2018. https://watson.brown.edu/costsofwar/files/cow/imce/papers/2018/Crawford_Costs%20of%20War%20Estimates%20Through%20FY2019%20.pdf.

Cuffari, Joseph V. *TSA Needs to Improve Management of the Quiet Skies Program (REDACTED)*. Washington, DC: Office of the Inspector General, Department of Homeland Security, 2020. https://www.oig.dhs.gov/sites/default/files/assets/2020-11/OIG-21-11-Nov20-Redacted.pdf.

Davis, Wanda. "Wanda (Wanda Frazier) Davis." LinkedIn, August 3, 2019. https://www.linkedin.com/in/wanda-davis-62b350b0/.

De Meo, Antonia Marie. *Stop the Virus of Disinformation: The Risk of Malicious Use of Social Media during COVID-19 and the Technology Options to Fight It*. Turin, Italy: United Nations Interregional Crime and Justice Research Institute (UNICRI), 2020. http://www.unicri.it/sites/default/files/2020-11/SM%20misuse.pdf.

Dean, Lisa S. *Security Threat Assessment for SIDA and Sterile Area Workers*. Washington, DC: Transportation Security Administration, 2004. https://www.dhs.gov/sites/default/files/publications/privacy_pia_sida_sw_0.pdf.

Defense Intelligence Agency. "HUMINT." Accessed December 17, 2020. https://www.dia.mil/Careers-Internships/Career-Fields/Human-Intelligence/#overview.

Department of Homeland Security. *Air Domain Surveillance and Intelligence Integration Plan*. Washington, DC: United States Department of Defense, Office of the Secretary of Defense, Office of the Director of National Intelligence, 2007. https://www.hsdl.org/?view&did=472112.

———. "Homeland Security Information Network (HSIN)." November 19, 2014. https://www.dhs.gov/homeland-security-information-network-hsin.

———. "Office of Intelligence and Analysis." June 18, 2015. https://www.dhs.gov/office-intelligence-and-analysis.

———. *Requests for Identities of U.S. Persons in Disseminated Intelligence Reports*. Washington, DC: Department of Homeland Security, 2020. https://www.intel.gov/assets/documents/702%20Documents/oversight/DHS_ICPG_107_1_Unmasking_Procedures_022420OCR.pdf.

———. "Secretary Nielsen Receives Operational Briefing on Israeli Security Technology, Delivers Remarks at the International Homeland Security Forum." June 12, 2018. https://www.dhs.gov/news/2018/06/12/secretary-nielsen-receives-operational-briefing-israeli-security-technology-delivers.

———. "The Intelligence Enterprise." August 8, 2019. https://www.dhs.gov/intelligence-enterprise.

———. TSA's Office of Intelligence and Analysis Has Improved Its Field Operations. Washington, DC: Department of Homeland Security Office of the Inspector General, 2017. https://www.oversight.gov/report/dhs/tsas-office-intelligence-and-analysis-has-improved-its-field-operations.Department of Justice. *Request for Records Disposition Authority*. Standard Form 115 (REV 3 91). College Park, MD: National Archives & Records Administration, 2010. https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0065/n1-065-10-025_sf115.pdf.

Director of National Intelligence. "IC Budget, What We Do." 2021. https://www.dni.gov/index.php/what-we-do/ic-budget.

———. *Intelligence Community Directive 204—National Intelligence Priorities Framework*. Washington, DC: Office of the Director of National Intelligence, 2021. https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf.

———. *Intelligence Community Directive 304—Human Intelligence*. Washington, DC: Office of the Director of National Intelligence, 2009. https://www.dni.gov/files/documents/ICD/ICD%20304.pdf.

———. *Intelligence Community Directive 900—Integrated Mission Management*. Washington, DC: Office of the Director of National Intelligence, 2013. https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives.

———. *(U) Domestic Violent Extremism Poses Heightened Threat in 2021*. Washington, DC: Office of the Director of National Intelligence, 2021. https://www.dni.gov/files/ODNI/documents/assessments/UnclassSummaryofDVEAssessment-17MAR21.pdf.

Department of the Army. *Human Intelligence Collector Operations*. Vol. FM 34-35, Field Manual 2-22. Washington, DC: Pentagon Library, 2006. https://www.loc.gov/rr/frd/Military_Law/pdf/human-intell-collector-operations.pdf.

District of Puerto Rico, U.S. Attorney's Office. "Twelve Current and Former TSA and Airport Employees Indicted for Smuggling Approximately 20 Tons of Cocaine." Department of Justice, February 13, 2017. https://www.justice.gov/usao-pr/pr/twelve-current-and-former-tsa-and-airport-employees-indicted-smuggling-approximatley-20.

Edbrook, C. D. "Principle of Deep Cover." *Studies in Intelligence* 5, no. Summer (1961): 1–31.

Evanina, William R. *National Counterintelligence and Security Center Strategic Plan, 2018–2022*. Washington, DC: National Counterintelligence and Security Center, 2018. https://www.odni.gov/files/NCSC/documents/Regulations/2018-2022-NCSC-Strategic-Plan.pdf.

Federal Bureau of Investigation. "Terrorist Screening Center." Accessed July 5 2021. https://www.fbi.gov/about/leadership-and-structure/national-security-branch/tsc.

———. "What We Investigate: Transnational Organized Crime." Accessed April 25, 2019. https://www.fbi.gov/investigate/organized-crime.

Fjeld, Christian T. "Hearings on the SolarWinds Hack and Possible Policy Responses." Insights Center, Mintz, February 23, 2021. https://www.mintz.com/insights-center/viewpoints/2236/2021-03-04-hearings-solarwinds-hack-and-possible-policy-responses.

Flashpoint. "Oversight of Intelligence Operations Begins with Collections Management." *Flashpoint* (blog). September 27, 2018. https://www.flashpoint-intel.com/blog/oversight-of-intelligence-operations-begins-with-collections-management/.

Franz, George J. “Beyond Desert Storm—Conducting Intelligence Collection Management Operations in the Heavy Division.” Monograph, Fort Leavenworth, KS, School of Advance Military Studies, United States Army Command and General Staff College, 1995. https://apps.dtic.mil/dtic/tr/fulltext/u2/a309837.pdf.

German, Mike. “Rethinking Intelligence: Interview with Erik Dahl.” Brennan Center for Justice, June 6, 2014. https://www.brennancenter.org/our-work/research-reports/rethinking-intelligence-interview-erik-dahl.

Glaun, Dan. “A Timeline of Domestic Extremism in the U.S., from Charlottesville to January 6.” Public Broadcasting Service, Frontline, April 21, 2021. https://www.pbs.org/wgbh/frontline/article/timeline-us-domestic-extremism-charlottesville-january-6/.

Goepner, Erik, and Trevor A. Thrall. “Time to Step Back from the War on Terror.” Cato Institute, October 26, 2017. https://www.cato.org/publications/commentary/time-step-back-war-terror.

Government Accountability Office. *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA’s Pipeline Security Program Management*. GAO-19-48. Washington, DC: Government Accountability Office, 2018. https://www.gao.gov/assets/700/696123.pdf.

———. *DHS Intelligence Analysis: Additional Actions Needed to Address Analytic Priorities and Workforce Challenges*. GAO-14-397. Washington, DC: Government Accountability Office, 2014. https://www.gao.gov/assets/670/663794.pdf.

Government Technology & Services Coalition’s. “CBP, ICE Bids to Join Intelligence Community Gain Traction.” Homeland Security Today, February 14, 2018. https://www.hstoday.us/federal-pages/odni/cbp-ice-bids-to-join-intel-community-gain-traction/.

Green, J. J. “City of Secrets: Estimated 10,000 People in DC Are Spies.” WTOP, June 17, 2019. https://wtop.com/j-j-green-national/2019/06/city-of-secrets-an-estimated-10000-dc-residents-are-spies-heres-how-they-blend-in/.

Greitzer, Frank L., Lars J. Kangas, Christine F. Noonan, Christopher R. Brown, and Thomas Ferryman. “Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis.” *Indiana University Press E-Service Journal* 9, no. 1 (Fall 2013): 106–138.

Grover, Jennifer, and Jessica Farb. *Aviation Security TSA Strengthened Foreign Airport Assessments and Air Carrier Inspections, but Could Improve Analysis to Better Address Deficiencies*. GAO-18-178. Washington, DC: Government Accountability Office, 2017. https://www.gao.gov/assets/690/688730.pdf.

GW Program on Extremism. “Capitol Hill Siege.” 2021. https://extremism.gwu.edu/Capitol-Hill-Cases.

Hart, Jeremiah J. “Strategic Mutual Aid Response to Terrorism: A New Approach.” Master’s thesis, Naval Postgraduate School, 2020. https://www.hsdl.org/?abstract&did=839423.

Haspel, Gina. “CIA Director Gina Haspel Speaks at Auburn University.” Central Intelligence Agency, April 18, 2019. https://www.cia.gov/stories/story/cia-director-gina-haspel-speaks-at-auburn-university/.

Heeley, Laicie, Amy Belasco, Mackenzie Eaglen, Luke Hartig, Tina Jonas, Mike McCord, and John Mueller. *Counterterrorism Spending: Protecting America while Promoting Efficiencies and Accountability*. Washington, DC: Henry L. Stimson Center, 2018. https://www.hsdl.org/?abstract&did=810501.

History.com Editors. “Reaction to 9/11.” History, August 7, 2019. https://www.history.com/topics/21st-century/reaction-to-9-11.

Inserra, David. “Here’s How Safe We Are 17 Years after 9/11.” The Heritage Foundation, September 11, 2018. https://www.heritage.org/homeland-security/commentary/heres-how-safe-we-are-17-years-after-911.

———. “Time to Privatize the TSA.” The Heritage Foundation, July 19, 2017. https://www.heritage.org/homeland-security/report/time-privatize-the-tsa.

Jackson, Matthew L. “America’s Three Domestic Threats and the Need for a Reform of Domestic Intelligence.” Master’s thesis, Naval Postgraduate School, 2020. https://calhoun.nps.edu/bitstream/handle/10945/66087/20Sep_Jackson_Matthew.pdf?sequence=1&isAllowed=y.

Joh, Elizabeth E. *Reclaiming “Abandoned” DNA: The Fourth Amendment and Genetic Privacy*. Vol. 100, no. 2. Chicago: Northwestern University Law Review, 2006. http://www.antoniocasella.eu/dnlaw/Joh_2006.pdf.

Jones, Seth G., Catrina Doxsee, and Nicholas Harrington. *The Escalating Terrorism Problem in the United States*. Washington, DC: Center for Strategic & International Studies, 2020. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200612_Jones_DomesticTerrorism_v6.pdf.

Kelly, John F. “Home and Away: DHS and the Threats to America.” Department of Homeland Security, April 18, 2017. https://www.dhs.gov/news/2017/04/18/home-and-away-dhs-and-threats-america.

Kimery, Anthony. “DNA Processing Carried Out by DHS S&T for FBI, Intel Agencies.” Biometric Update, January 14, 2019. https://www.biometricupdate.com/201901/dna-processing-carried-out-by-dhs-st-for-fbi-intel-agencies.

Landler, Mark, and Eric Schmitt. "Terrorist Threat 'More Fluid and Complex than Ever,' White House Says." *New York Times*, sec. United States, October 4, 2018. https://www.nytimes.com/2018/10/04/us/politics/trump-counterterrorism-strategy.html.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. 7th ed. Los Angeles: QC Press, 2017.

Majority Staff of the House Homeland Security Committee. *Reviewing the Department of Homeland Security's Intelligence Enterprise*. Washington, DC: Homeland Security Committee, 2016. https://www.hsdl.org/?view&did=797351.

McAleenan, Kevin K. *The DHS Strategic Plan Fiscal Years 2020–2024*. Washington, DC: Department of Homeland Security, 2019. https://www.dhs.gov/publication/department-homeland-securitys-strategic-plan-fiscal-years-2020-2024.

McGarrity, Michael C. "Confronting the Rise of Domestic Terrorism in the Homeland." Federal Bureau of Investigation, May 8, 2019. https://www.fbi.gov/news/testimony/confronting-the-rise-of-domestic-terrorism-in-the-homeland.

McGarrity, Michael C., and Calvin A. Shivers. "Confronting White Supremacy, Statement before the House Oversight and Reform Committee, Subcommittee on Civil Rights and Civil Liberties Washington, D.C." Federal Bureau of Investigation, June 4, 2019. https://www.fbi.gov/news/testimony/confronting-white-supremacy.

McKinney, India. "TSA's Roadmap for Airport Surveillance Moves in a Dangerous Direction." Electronic Frontier Foundation, December 7, 2018. https://www.eff.org/deeplinks/2018/12/tsas-roadmap-airport-surveillance-moves-dangerous-direction.

Medina, Brenda, and Thomas Frank. "TSA Agents Say They're Not Discriminating against Black Women, but Their Body Scanners Might Be." ProPublica, April 17, 2019. https://www.propublica.org/article/tsa-not-discriminating-against-black-women-but-their-body-scanners-might-be.

Miller, Greg. "The CIA Unveils a Radically New Org Chart." *Washington Post*, sec. Military, October 1, 2015. https://www.washingtonpost.com/news/checkpoint/wp/2015/10/01/the-cia-unveils-a-radically-new-org-chart/.

Mueller, Robert S. III. "The FBI Transformation since 2001." Federal Bureau of Investigation, September 14, 2006. https://www.fbi.gov/news/testimony/the-fbi-transformation-since-2001.

Mullen, Marisa. “Transportation Security Administration Transition to Department of Homeland Security; Technical Amendments Reflecting Organizational Changes.” National Archives, Federal Register, August 19, 2003. https://www.federalregister.gov/documents/2003/08/19/03-20927/transportation-security-administration-transition-to-department-of-homeland-security-technical.

National Archives and Records Administration. “Transportation Security Administration.” Federal Register. Accessed December 3, 2020. https://www.federalregister.gov/agencies/transportation-security-administration.

National Commission on Terrorist Attacks. *The 9/11 Commission Report*. Washington, DC: National Commission on Terrorist Attacks, 2004. https://govinfo.library.unt.edu/911/report/911Report.pdf.

National Counterintelligence Executive. *(U) U.S. Insider Threat Security Classification Guide 2013*. Version 1. Washington, DC: Office of the Director of National Intelligence, 2013. https://www.dni.gov/files/documents/FOIA/DF-2016-00161.pdf.

National Counterterrorism Center. *Terrorist Identities Datamart Environment (TIDE)*. Washington, DC: Office of the Director of National Intelligence, 2017. https://www.dni.gov/files/NCTC/documents/features_documents/TIDEfactsheet10FEB2017.pdf.

National Security Staff. *Transnational Organized Crime: A Growing Threat to National and International Security*. Washington, DC: White House, 2011. https://obamawhitehouse.archives.gov/node/60577.

Negroponte, John D. *Director of National Intelligence*. Washington, DC: Director of National Intelligence, 2006. https://fas.org/irp/dni/dni020706.pdf.

Office of Public Affairs. “Kenyan National Indicted for Conspiring to Hijack Aircraft on Behalf of the Al Qaeda-Affiliated Terrorist Organization Al Shabaab.” December 16, 2020. https://www.justice.gov/opa/pr/kenyan-national-indicted-conspiring-hijack-aircraft-behalf-al-qaeda-affiliated-terrorist.

Office of the Director of National Intelligence. *Annual Threat Assessment of the U.S. Intelligence Community*. Washington, DC: Office of the Director of National Intelligence, 2021. https://www.hsdl.org/?abstract&did=852427.

———. “Members of the IC.” March 28, 2019. https://www.dni.gov/index.php/what-we-do/members-of-the-ic.

———. “Organization.” Accessed April 25, 2019. https://www.odni.gov/index.php/component/content/article?id=341&Itemid=583.

———. “Transnational Organized Crime.” June 2011. https://www.dni.gov/index.php/who-we-are/organizations/ise/archive/additional-resources/2146-transnational-organized-crime.

Office of the Historian. “Milestones: 1945–1952 National Security Act of 1947.” Accessed December 12, 2020. https://history.state.gov/milestones/1945-1952/national-security-act.

Office of the Inspector General. *TSA Can Improve Aviation Worker Vetting (Redacted)*. OIG-15-98. Washington, DC: Department of Homeland, 2015. https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-98_Jun15.pdf.

———. *TSA Needs to Improve Management of the Quiet Skies Program (Redacted)*. OIG-21-11. Washington, DC: Department of Homeland Security, 2020. https://www.oig.dhs.gov/sites/default/files/assets/2020-11/OIG-21-11-Nov20-Redacted.pdf.

———. *TSA’s Office of Intelligence and Analysis Has Improved Its Field Operations*. Report No. OIG-17-107. Washington, DC: Department of Homeland Security, 2017. https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-107-Sep17.pdf.

Parfomak, Paul W., and Chris Jaikaran. *Colonial Pipeline: The DarkSide Strikes*. CRS Report No. IN11667. Washington, DC: Congressional Research Service, 2021. https://crsreports.congress.gov/product/pdf/IN/IN11667.

Pekoske, David P. *Insider Threat Roadmap 2020*. Washington, DC: Transportation Security Administration, 2020. https://www.tsa.gov/sites/default/files/3597_layout_insider_threat_roadmap_0424.pdf.

———. “Keeping Our Skies Secure: Oversight of the TSA.” Transportation Security Administration, September 5, 2018, https://www.tsa.gov/news/press/testimony/2018/09/05/keeping-our-skies-secure-oversight-tsa.

Potapov, Serge. *Privacy Impact Assessment for the Insider Threat Unit Database*. Washington, DC: Department of Homeland Security, 2018. https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsa048-april2018.pdf.

Priest, Dana, and William M. Arkin. “The Secrets Next Door.” *Washington Post*, sec. Investigative, July 21, 2010. https://www.washingtonpost.com/investigations/top-secret-america/2010/07/21/secrets-next-door/.

Rabasa, Angel, Christopher M. Schnaubelt, Peter Chalk, Douglas Farah, Gregory Midgette, and Howard J. Shatz. *Counternetwork Countering the Expansion of Transnational Criminal Networks*. Santa Monica, CA: RAND, 2017. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1481/RAND_RR1481.pdf.

Randol, Mark A. *Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress*. CRS Report No. R40602. Washington, DC: Congressional Research Service, 2010. https://www.hsdl.org/?abstract&did=27362.

Reagan, Ronald. "Executive Order 12333—United States Intelligence Activities." National Archives, December 4, 1981. https://www.archives.gov/federal-register/codification/executive-order/12333.html.

Rosenblum, Todd. "Homeland Intelligence: The Unique Community within the Community." *The Cipher Brief* (blog). October 9, 2016. https://www.thecipherbrief.com/column_article/homeland-intelligence-the-unique-community-within-the-community.

———. "Inside DHS' Intelligence Mission." The Cipher Brief, August 29, 2018. https://www.thecipherbrief.com/column_article/inside-dhs-intelligence-mission.

Russell, William. *Aviation Security TSA Has Policies that Prohibit Unlawful Profiling but Should Improve Its Oversight of Behavior Detection Activities*. GAO-19-490T. Washington, DC: Government Accountability Office, 2019. https://www.gao.gov/assets/700/699485.pdf.

Sadler, Steve. "TSA Secure Flight Program." National Security Administration, September 18, 2014. https://www.dhs.gov/news/2014/09/18/written-testimony-tsa-house-homeland-security-subcommittee-transportation-security.

Sales, Nathan A. "Countering Iran's Global Terrorism." Department of State, November 13, 2018. https://www.state.gov/countering-irans-global-terrorism/.

Schneier, Bruce. "Why Are We Spending $7 Billion on TSA?." CNN, June 5, 2015. https://www.cnn.com/2015/06/05/opinions/schneier-tsa-security/index.html.

Swan, Betsy Woodruff. "DHS Looking at Tracking Travel of Domestic Extremists." POLITICO, March 23, 2021. https://www.politico.com/news/2021/03/23/homeland-security-domestic-extremists-477658.

Temple-Raston, Dina. "The State of Intelligence: Fifteen Years after 9/11." Council on Foreign Relations, September 12, 2016. https://www.cfr.org/event/state-intelligence-fifteen-years-after-911.

Thompson, Bennie G. "Chairman Thompson: TSA and FBI Must Add Suspected Domestic Terrorists to No-Fly List and Keep Them off Planes." House Committee on Homeland Security, January 7, 2021. https://homeland.house.gov/news/press-releases/chairman-thompson-tsa-and-fbi-must-add-suspected-domestic-terrorists-to-no-fly-list-and-keep-them-off-planes.

Tracey, Matthew. *Privacy Impact Assessment Update for the TSA Encounter Analysis Branch*. Washington, DC: Department of Homeland Security, 2019. https://www.dhs.gov/sites/default/files/publications/privacy-pia-tsaeab-july2019.pdf.

Transportation Security Administration. *Budget Overview: Fiscal Year 2020 Congressional Justification*. Washington, DC: Department of Homeland Security, 2020. https://www.dhs.gov/sites/default/files/publications/19_0318_MGMT_CBJ-Transportation-Security-Administration_0.pdf.

———. "Intelligence Operations Specialist—SV-0132-J—Career's, Women's Job List." April 8, 2015. https://www.womensjoblist.com/jobs/21478890/Intelligence-Operations-Specialist-SV-0132-J/.

———. "Leadership and Organization." Accessed July 5, 2021. https://www.tsa.gov/about/tsa-leadership.

———. "Operations Support—Executive Assistant Administrator." Accessed July 5, 2021. https://www.tsa.gov/leader-bios/operations-support.

———. "Recurrent Vetting." Accessed July 5, 2021. https://www.tsa.gov/travel/frequently-asked-questions/recurrent-vetting.

———. "Transportation Security Administration Representative (TSAR)." February 14, 2019. https://diversityjobs.com/jobsearch/display/720379298?utm_medium=social&utm_source=facebook.

———. "TSA by the Numbers." Last updated May 19, 2021. https://www.tsa.gov/news/press/factsheets/tsa-numbers.

———. "TSA Transportation Security Operations Center: Still on Watch." *Transportation Security Administration* (blog). May 7, 2014. https://www.tsa.gov/blog/2014/05/07/tsa-transportation-security-operations-center-still-watch.

Trump, Donald J. *National Security Presidential Memorandum-9*. Washington, DC: White House, 2018. https://www.dhs.gov/sites/default/files/publications/NSPM-9%20Implementation%20Plan.pdf.

———. *National Strategy for Aviation Security of the United States of America*. Washington, DC: White House, 2018. https://www.hsdl.org/?abstract&did=821736.

———. *National Strategy for Counterterrorism of the United States of America*. Washington, DC: White House, 2018. https://www.dni.gov/files/NCTC/documents/news_documents/NSCT.pdf.

U.S. Congress. House of Representatives. *Examining TSA's Global Efforts to Protect the Homeland from Aviation Threats and Enhance Security at Last-Point-of-Departure Airports: Hearing before the Subcommittee on Transportation Security of the Committee on Homeland Security*. 114th Cong., 1st sess., December 8, 2015. https://www.hsdl.org/?abstract&did=806622.

United States Attorney's Office Northern District of California, United States Department of Justice, The. "Former TSA Transportation Security Officer Sentenced to 21 Months in Prison for Circumventing Security Checkpoint Screening." Accessed May 24, 2021. https://www.justice.gov/usao-ndca/pr/former-tsa-transportation-security-officer-sentenced-21-months-prison-circumventing.

United States Senate. *Unifying DHS Intelligence Components Act*. Washington, DC: United States Government Publishing Office, 2020. https://www.hsdl.org/?abstract&did=853607.

Wagner, Caryn A. *Office of Intelligence and Analysis Strategic Plan—Fiscal Year 2011–Fiscal Year 2018*. Washington, DC: Office of Intelligence and Analysis, Department of Homeland Security, 2011. https://www.dhs.gov/xlibrary/assets/ia-fy2011-fy2018-strategic-plan.pdf.

Walker, Summer, Walter Kemp, Mark Shaw, and Tuesday Reitano. *The Global Illicit Economy: Trajectories of Transnational Organized Crime*. Geneva, Switzerland: Global Initiative against Transnational Organized Crime, 2021. https://globalinitiative.net/wp-content/uploads/2021/03/The-Global-Illicit-Economy-GITOC-Low.pdf.

Wilder, Ursula M. "Why Spy?, The Psychology of Espionage." *Studies in Intelligence* 61, no. 2 (June 2017): 1–35.

Winter, Jana, and Jenn Abelson. "TSA Says It No Longer Tracks Regular Travelers like Terrorists." *The Boston Globe*, December 15, 2018. https://www.bostonglobe.com/news/nation/2018/12/15/curtails-quiet-skies-passenger-surveillance/2lRAv2AwjGpUcgq08mHaPM/story.html.

Wirth, Kevin E. *The Coast Guard Intelligence Program Enters the Intelligence Community: A Case Study of Congressional Influence on Intelligence Community Evolution*. Washington, DC: National Defense Intelligence College, 2007. https://apps.dtic.mil/sti/pdfs/ADA476640.pdf.

Wray, Christopher. "Oversight of the Federal Bureau of Investigation." Federal Bureau of Investigation, July 23, 2019. https://www.fbi.gov/news/testimony/oversight-of-the-federal-bureau-of-investigation-072319.

Zegart, Amy, and Michael Morell. “Spies, Lies, and Algorithms.” *Foreign Affairs*, May 28, 2019. https://www.foreignaffairs.com/articles/2019-04-16/spies-lies-and-algorithms.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California